THE EMAIL SECURITY GUIDE

BY GAVIN PHILLIPS

The Email Security Guide

Written by Gavin Phillips

Table of Contents

Chapter 1: Why Do You Need Secure Email?

Welcome to the MakeUseOf Email Security Course. In this course you'll learn how to lock down your inbox and **secure one of the single most important digital assets in your life**.

Why Do You Need Secure Email?

Let's not beat about the bush; **why do you need secure email**?

Secure email is a cornerstone of a happy online existence. Every time you sign up for a new online service, you use your email address. When you forget a password, you use your email address to reset it. Your inbox contains addresses, phone numbers, personal information (about you and others!), and much more.

And if an attacker makes their way into your email account, if they manage to break into and take over your account, they can almost instantaneously begin attacking your other accounts. Think; your Amazon, your Twitter, your Netflix, your online banking, and more.

Email is deeply ingrained in society. The average office worker receives over 120 emails per day and sends out 40 in return. Email has become synonymous with an active, mobile workforce, too. DMR, a digital marketing fact curation site, **states** that 86 percent of professionals name email as their favorite communication tool, while 66 percent of us read email on our mobile devices.

The ease of access, the sheer volume, and the now ubiquitous nature of email does mean that as a society, complacency sets in. The combination of human error, spam and phishing email, and other security vulnerabilities mean your email account is more vulnerable than you realize. Furthermore, the constant barrage of security news—breaches, failings, vulnerabilities, insecurities, and more—leads to dissonance. Simply put, we stop caring when there is too much noise.

But email account security is serious. That's why in this guide you are going to learn about:

- Why email encryption is important and why email isn't secure.
- Common email security mistakes, spotting scam emails, and creating the perfect password.
- Learn all about turning on 2FA, using a VPN, and how to check your email securely.
- How do you choose a secure email provider? How do you check your emails in public securely?
- Different encryption types, including how to encrypt Outlook, whether to use OpenPGP, and which emails you should encrypt.
- Can your instant messaging service safely replace your secure email account? And Is that even practical?

You will find something new to learn in each section of this email security guide!

Email Encryption Is Important

Here's something for you to consider.

Where is your email vulnerable? Like, the actual locations where your email is vulnerable to compromise. There are four main locations when someone else can grab your email:

- **Your devices.** The device you read your email on, be that a smartphone, desktop, or so on.
- **The network.** The network means the internet connection you're using to access your email account.
- **The server.** The server is where emails move from your account to your recipients; an online email server is also where your emails store so you can access them from anywhere, on any computer.
- **Your recipient device.** The device your recipient is reading your email on.

Did you get all four? Within those four locations are the overwhelming majority of places where a malicious party could access your email. The internet is more secure than ever before, with most sites and services now using the more secure HTTPS standard rather than regular HTTP. However, even with the additional security offered by HTTPS, wouldn't you prefer an additional layer of protection?

That's where email encryption steps in. Just as sending an email has never been easier, adding an extra layer of encryption to your mail is just as simple. Encryption essentially wraps your email in a new layer of near-impenetrable data that stops a malicious party reading the contents of your email. (I say "near-impenetrable" as encryption comes in different strengths, encryption isn't guaranteed to stay secure forever, and some encryption algorithms are already vulnerable.)

For instance, if you send a regular email containing sensitive information, the email passes through a series of servers. If an attacker has compromised the server, there's a strong chance they can read everything passing through the server. If you sent that same sensitive email with a layer of encryption, the attacker would have very little chance of reading the contents due to the difficulty of removing the additional security layer.

(You will learn more about encrypting your emails later in this guide.)

The stakes are high. The attacker is likely to move swiftly on to other, less secure emails rather than attempting to attack and decrypt your private information. The effort isn't worth it—unless you are a very high worth individual, of course.

Email Isn't Secure

Always remember one thing: **your email account isn't secure**, so don't assume it is. The assumption of security is a major issue for all email users. The main email protocol (a protocol is a set of rules that dictate how something acts, in this case, how email is sent across the internet), SMPT (Simple Mail Transfer Protocol), has no integrated security mechanisms.

Yup, that's right. The main source of communication around the entire globe has no inherent security.

Here's **an article regarding email security protocols** if you would like to understand more. Protocols are a little dry, but they do underpin your email security, so **I would advise reading the article** for some interesting email security background information.

Of course, email providers and servers have security built-in. Over the years, it became painfully obvious that using something as ubiquitous as email without security was bonkers. Security varies between email providers and email clients, so don't assume you are protected—it might not be the case.

Furthermore, this illustrates why taking the time to encrypt your email is so important.

Before reading the next chapter:

- Take a look at the email security protocol article linked above.

Chapter 2: Do You Make These Common Email Security Mistakes?

One of the biggest problems facing us as regular email users is something basic—something that starts at home. That's right; **it's us.** The human connection is a constant thorn in the side of security and tech companies. There is no counting for what an individual can and will click on, or a weak password, or a poorly configured, insecure computer.

In this chapter, you're going to learn about the most common email security mistakes---**and how you can avoid making them**.

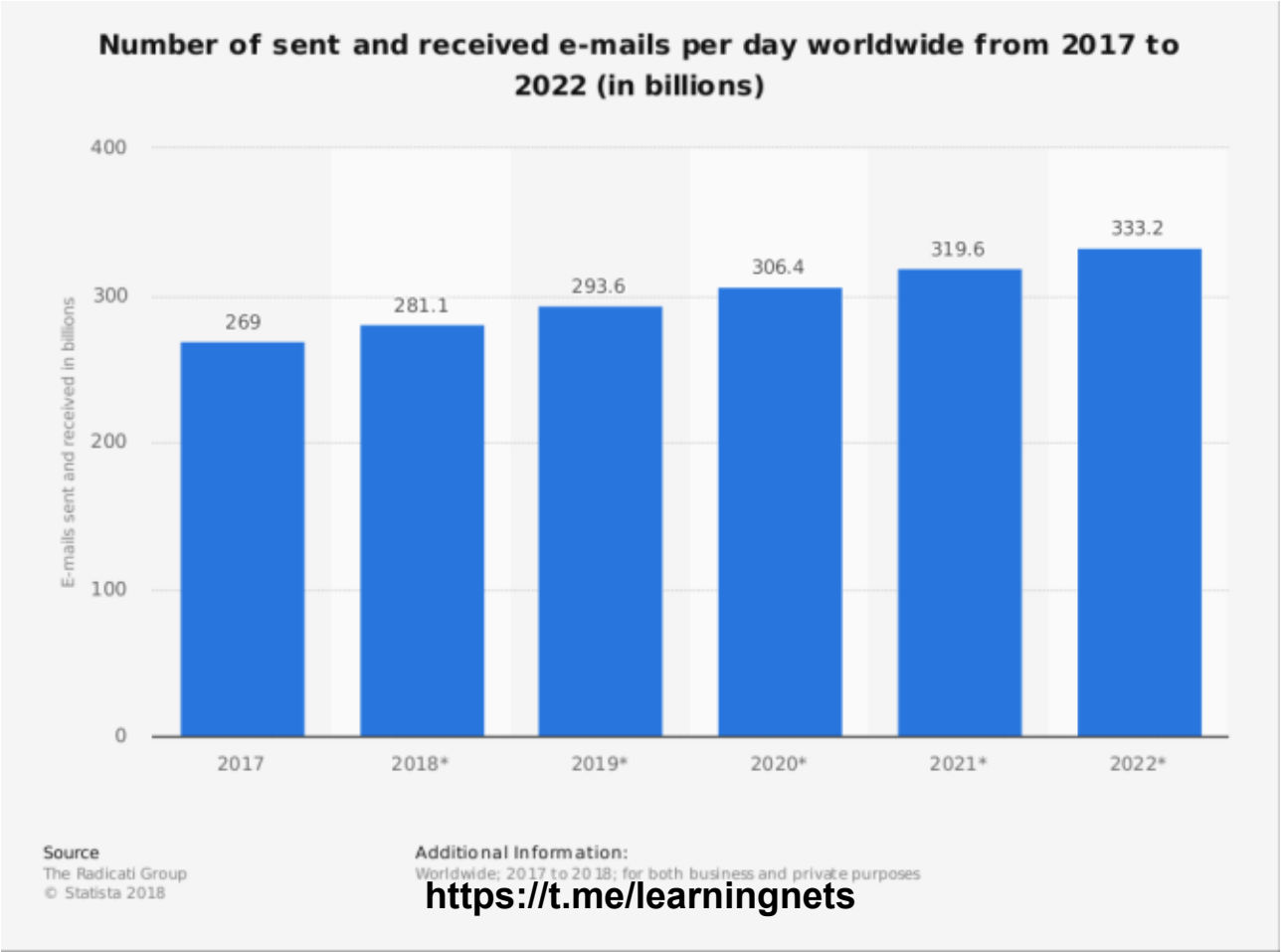
Do You Make These Common Email Security Mistakes?

When I say common email security mistakes, this is what I mean:

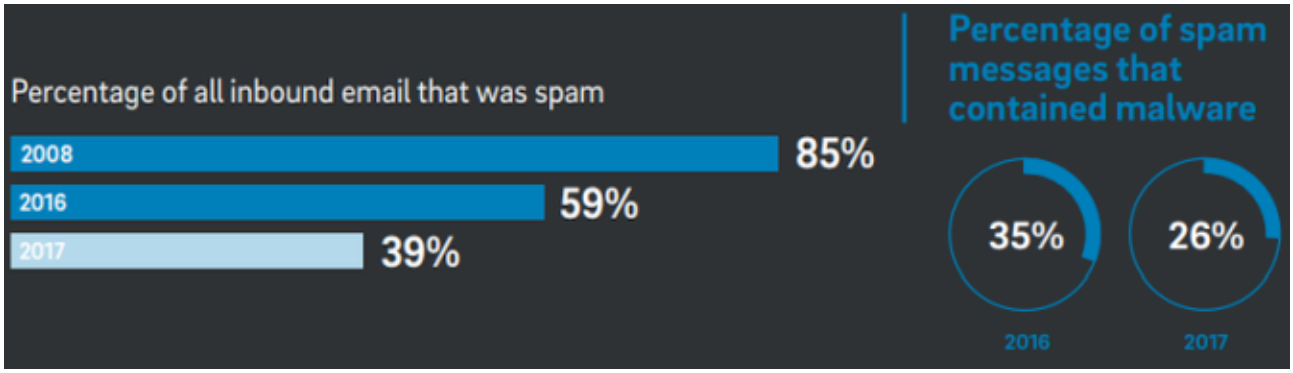
- Clicking on links in suspicious emails
- Poor spam filtering leading to an influx of malicious email
- Opening unsolicited email attachments
- Weak and reused passwords

How to Spot Suspicious Scam and Phishing Emails

According to Statista, over 280 billion emails are sent and received every day. Depending on where you find your stats and definitions, spam email accounts for anywhere between 5 percent to 45 percent of all email sent every day. Statista puts this figure **as high as 55 percent**, whereas the **2018 Trustwave Global Security Report** puts it as low as 39 percent.



Your inbox, then, is a hotbed of potential spam email. Within the dietary pills and Nigerian Prince emails lurk another kind of issue. In amongst the spam are cryptocurrency blackmails, extortion attempts, malicious invoices for regular internet services, and much more. However, they're not always easy to spot.



Don't be downhearted. Just today I was sent a fake Amazon Prime invoice with a very similar renewal date to my own, and I almost clicked it out of confusion. And that confusion is what spammers, scammers and otherwise rely on. Casting doubt in the hope you click a link or download a file you really shouldn't.

There are five things you can do to quickly verify whether the email sent to you from Amazon, Netflix, or your bank are the real deal.

1. **Check the sender email address.** Depending on the level of sophistication, the email address won't correlate to the institution allegedly sending it. If the sender email address for a supposed bank notification is "awesomehotstuff76@hotmail.com" you should be in no doubt that someone is attempting to scam you.

2. **Grammar and Spelling.** It is trivially easy to spoof the sender email address to match an official account. The second major giveaway is the language and grammar in use. Are the language and grammar accurate? Is your name and title correct? Does the language and tone of the email sound strange? Misspellings, poor grammar, and completely incorrect information are giveaways that something is afoot.

3. **URGENT.** What is the subject matter? Is it **"URGENT: Your Account will XYZ"**? Scammers and spammers know the best way to get into your mind is to use uncertainty. The uncertainty of an account in arrears, an unpaid bill, an outstanding old debt, or an unexpected account renewal notice is enough to grab the attention of most users (see my above experience with an Amazon phishing email for a prime example).

4. **Attachments.** Emails with unexpected attachments are a big red flag. A seemingly harmless attachment can carry malware to infect your system.

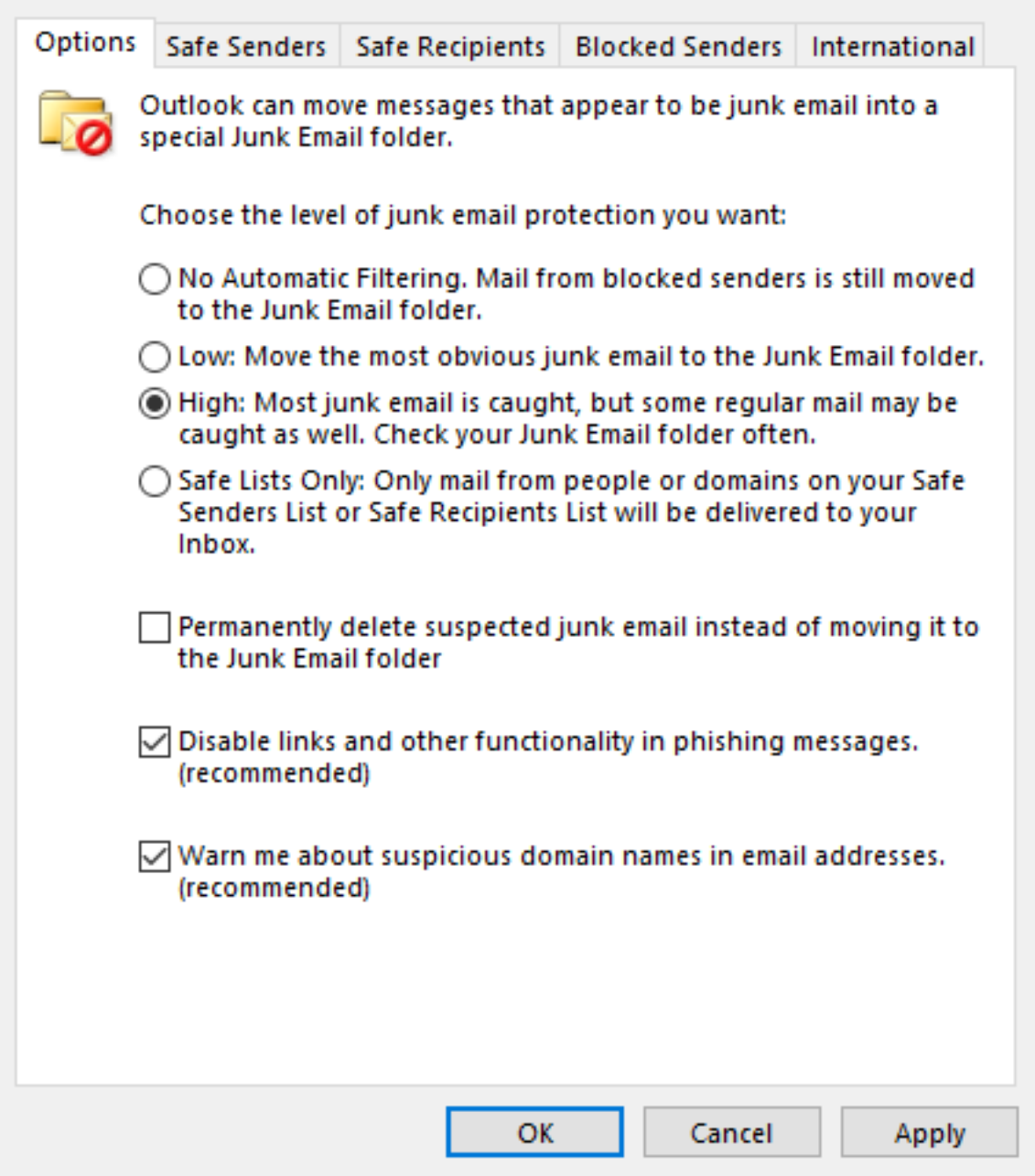
5. **Links.** The same goes for an email hyperlink. Scammers set up phishing sites that mimic login portals to steal your credentials. Don't follow any links from an unsolicited email.

The list isn't exhaustive. Scammers come up with new ways to trick unsuspecting users all the time. Did you know that it takes around 12.5 million spam emails to get one response? It sounds like a huge amount, but considering the billions of spam email sent every day, that still means around 10,000 people every day lose their credentials, install malware, send money to Nigeria, and respond to cryptocurrency scams.

MakeUseOf's Christian Cawley has some **more tips on spotting malicious phishing emails**, with some handy examples, too.

Turn Up Your Spam Filter

Your email account has a spam filter. The filter checks incoming email from known spam addresses, for spammy content, malicious attachments, and spammy subject matter bars and sends it directly to your spam box.



Some filters are better than others. At other times, you need to tweak your spam filter settings to block the rubbish before it hits your inbox. Here's how you **tweak your filters in Gmail to avoid unwanted incoming spam**, while **Outlook users can learn about adjusting their junk filters** right here.

Email Account Password

Modern life requires online accounts. Online accounts require passwords. Passwords require attention because they're key to stopping any attacker intruding into your account.

Password management is tricky, due to the number of accounts and the difficulty required to create a strong enough unique password that you can actually remember. Deep down, in your digital heart, you know that reusing your basic "hunter2" password is wrong. But it makes life easy. The problem is that "hunter2" is a weak password that an attacker can crack in no time at all.

So, what's the key to making a secure, unique password?

To get started, consider the following:

- It **must be longer** than eight characters.
- It **must not** use any identifying information: birthdays, pet names, birthplaces, etc.
- **Don't use** dictionary words; they're too easy to match.
- You **should** use a combination of letters, numbers, and symbols.

An ideal password looks like this:

- Zwb2=<UwrP77"?ra
- a%6HBT<*D[9>4z{p
- Z982eyG}`z%pF"N.

This is a completely random string of upper- and lower-case letters, numbers, and symbols. It has no link to my person at all, and is also 16 characters in length. It will take a password cracker a long time to break through. Long enough that someone will give up and move onto other, easier targets.

Use a Password Manager

The second biggest security boost you can give yourself and your email security is using a secure password manager. A password manager securely stores your passwords. Depending on the password manager, you copy your password across, or the password manager automatically inserts the correct password for the account in question.

There are a fair few password management tools out there, so check out the **MakeUseOf guide to choosing the right password manager** for your needs.

Before reading the next chapter:

- **Check** your inbox for any scam or spam emails (don't click on them though!)
- **Check** your email provider and see what level your spam filter is set too.
- **Think** about your passwords; are they strong enough, and could you use a password manager?

Chapter 3: How to Use Your Email Account Securely

This chapter is all about accessing and using your email securely, be that in your home or while connected to a free Wi-Fi connection in your favorite cafe.

How to Use Your Email Account Securely

More than 50% of all email **is opened** on a mobile device. Moreover, mobile email users check their email around three times more than desktop users. In the hyper-connected world, checking your email on the go is a simple yet effective productivity tip. It isn't even a productivity tip; it is the easiest way to stay connected to family, friends, work, and everything else in-between.

It is important, then, to keep all of your devices secure, be that a smartphone, laptop, tablet, or desktop. Here are six things for you to consider:

- **Make sure you set a secure device password**. Your device password should not use a birthday, phone number, or anything easily linked to you. Ideally, you can use a combination of letters and numbers, like a proper password, or even a passphrase (an easily remembered phrase is a much longer device key than a single word).
- **Avoid unsecured free public Wi-Fi**. Many places offer free public Wi-Fi for their clients or guests. If you don't have to sign into the Wi-Fi network using a password, the connection is insecure, and your internet traffic could be vulnerable to attack.
- **Use a Virtual Private Network (VPN)**. If you do have to use an unsecured free Wi-Fi network, using a VPN is a vital security step. Using a VPN creates a private tunnel between your device and the VPN provider server, making sure no one can snoop on your data.
- **Regular antimalware scans**. You can go to great lengths to use a secure email provider, but it won't matter a jot if an attacker installs keylogging or credential-stealing malware on your system. Scan your system regularly with **Malwarebytes Antimalware** (available for Windows, macOS, iOS, and Android), or better yet, upgrade to the premium version for live system protection. (Here are **five excellent reasons to consider upgrading to Malwarebytes Premium**!)
- **Update your system**. Install system updates. Sure, they can arrive at inconvenient times, but it is a smaller irritation than someone hacking your accounts with credentials stolen directly from you.
- **Turn on 2-Factor Authentication**. 2-Factor Authentication, or 2FA, adds another security layer to your account, sending a limited-use code to a separate device that you enter after your password. There are tips on using 2FA in the next inbox security lesson.
- **Add encryption**. If your current email provider doesn't support additional encryption levels, consider switching providers. If that isn't an option, a third-party encryption utility is what you need.

About that last point, "Add encryption." You might note that I've not talked about third-party encryption utilities. Oh, you guessed it; **encryption tips and tools are covered soon!**

Sign Up for a VPN

The third point on the how to check your email securely list above is “Use a Virtual Private Network.” You might have already heard the term “VPN.” Many people use a VPN to access video content in their native country when traveling abroad. That isn’t all VPNs are useful for, though. A VPN is a handy and cheap (sometimes free, but more on that in a moment) way to increase your security with very little effort. Here’s why:

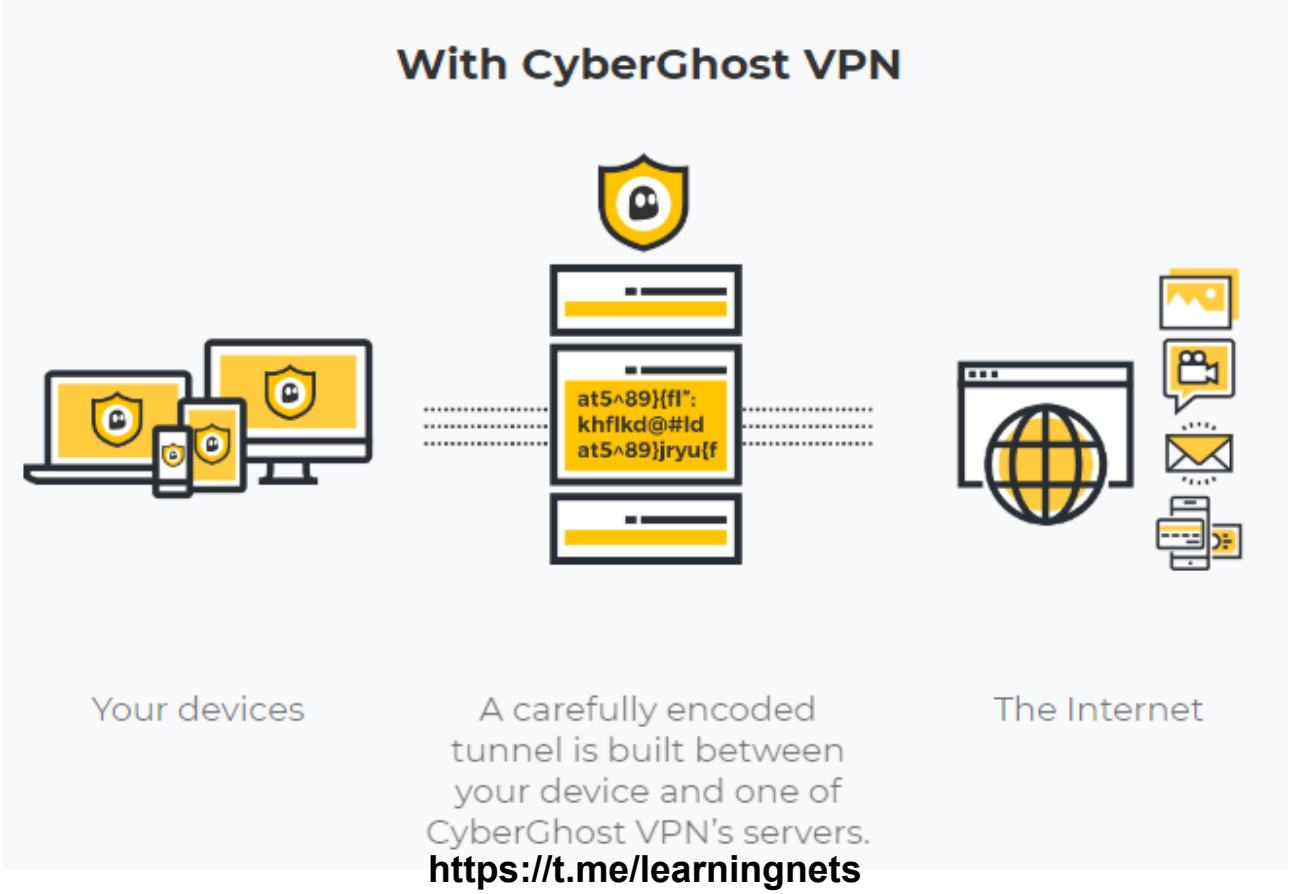
- When you browse the internet, your device sends the data to your internet service provider (ISP), and the ISP routes the data to the correct website. The ISP and the website know where you are and in theory can read the data in transit. Whereas,
- A VPN creates a tunnel between your device and the VPN providers private server. All of the traffic from your device routes through the VPN tunnel first before emerging from the VPN provider server. You can choose the VPN server location, too, making your traffic appear as it was coming from an alternative location.

The VPN tunnel is encrypted, protecting your data from any prying eyes between your device and the VPN server.

However, a VPN doesn’t directly encrypt or secure your emails. Using a VPN isn’t like encrypting an email directly within your email client or using a third-party encryption tool. Data transiting between your device and the VPN server is private and secure, but once it leaves the VPN server it is once again “in the wild.”

Use a Paid-For VPN Subscription

Now, I said “sometimes free.” Why only “sometimes,” you might wonder? Well, the old internet adage goes “if you’re not paying for the product, you are the product.” It is a model we see with Google, Facebook, and countless other free internet services. VPNs are no different. Truly securing your connection does come at a small cost, and a **paid VPN always trumps a free one**.



Luckily, there are numerous excellent VPN providers available that cost very little while providing an exemplary service. MakeUseOf **strongly recommends CyberGhost** for their commitment to privacy, performance, and flexibility. **I use it myself!**

That said, not all free VPNs are doom and gloom. Many free VPNs will absolutely do in a pinch, offering a range of download options, server locations, and privacy settings. MakeUseOf's Ben Stegner has tested some of the **best unlimited free VPNs you can lay your hands on**, while Christian Cawley regularly updates the MakeUseOf **guide to the best VPNs, both paid and free**.

How Do I Use a VPN?

Once you decide on a VPN provider you will download their VPN software or app to your device. Before checking your emails when connected to a free Wi-Fi connection, fire up the VPN and connect to a secure server, then open your email account. Your traffic remains secure from malice! Remember, you can use your VPN to encrypt your web traffic at all times, not just when you use a public Wi-Fi connection.

Many of the staff at MakeUseOf use a VPN at all times for the additional security and privacy.

Before reading the next chapter:

- **Think** about the ways you can use email securely and how you currently check your inbox.
- **Consider** updating and improving your device password; This was covered earlier in the guide.
- **Sign up** for a reputable VPN; be that a free VPN to figure out how they work or a paid option, a VPN gives you an instant security boost.
- **Check** your system for updates. If you have a pending system update, save your work and important documents, create a system restore point, then install it!

(Unsure about system restore points? Read "4. Enable Restore Point" in Joel's article looking at **what you should do before every Windows Update**. It is a great read with information for the frequent updates!).

Chapter 4: How to Choose a Secure Email Provider

This chapter is all about secure email providers: how you choose a provider, what the most secure email clients are, how you enable 2FA account security, if you can stop scammers from spoofing your email address, and why email security (like all cybersecurity) **is similar to a really delicious cake**.

Choosing a Secure Email Provider

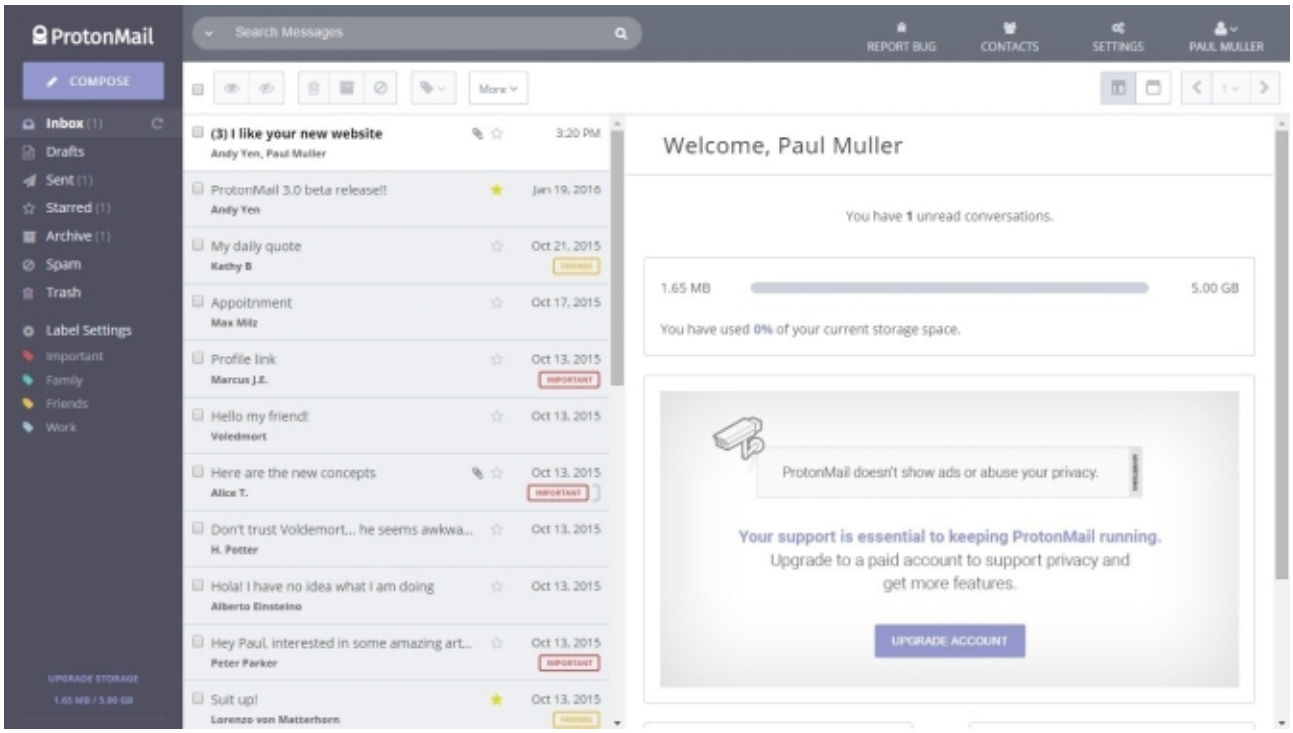
Choosing a secure email provider is easier than you think. There's a good reason for that. Despite the numerous reports of breaches, vulnerabilities, hacks, and so on, the average internet user has never been safer in the "modern" internet era.

There are numerous secure email providers out there. You have two questions to answer: What level of protection do you need? And how much are you willing to pay? You want your email client (the place you read your email) to be secure. You want your email to be secure in transit, too, using powerful encryption to protect your information further. You also don't want to break the bank, and in reality, you don't need to.

Several excellent secure email services offer end-to-end encryption for your emails. End-to-end encryption means protection for your email from the moment you hit send to the moment your recipient opens it. (What happens on your recipient device is, as you read at the start of this guide.)

Unfortunately, Outlook and Gmail don’t offer “end to end” encryption as standard. But, keep reading to find out how you can add this functionality in Outlook—and why you cannot do the same in Gmail.

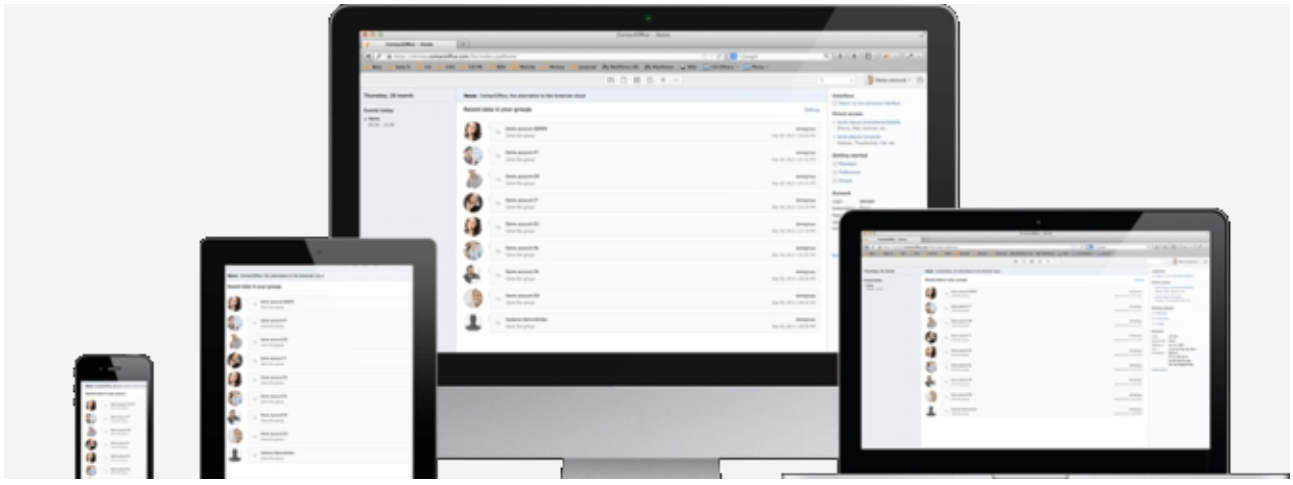
1. ProtonMail



ProtonMail is a free, open-source encrypted email provider. ProtonMail has a web client and apps for iOS and Android. How secure is ProtonMail? Well, unless your recipient has your email password, they cannot open your email. At all, ever. Even ProtonMail cannot (and will not) open your email, in any eventuality. Want another boost to your email security confidence? ProtonMail is based in Switzerland, one of the single-best countries for protecting private user data.

Unsure about switching from Gmail to ProtonMail? MakeUseOf's Editor in Chief Joel Lee **takes a closer look at which email provider is best for your needs**.

2. Mailfence

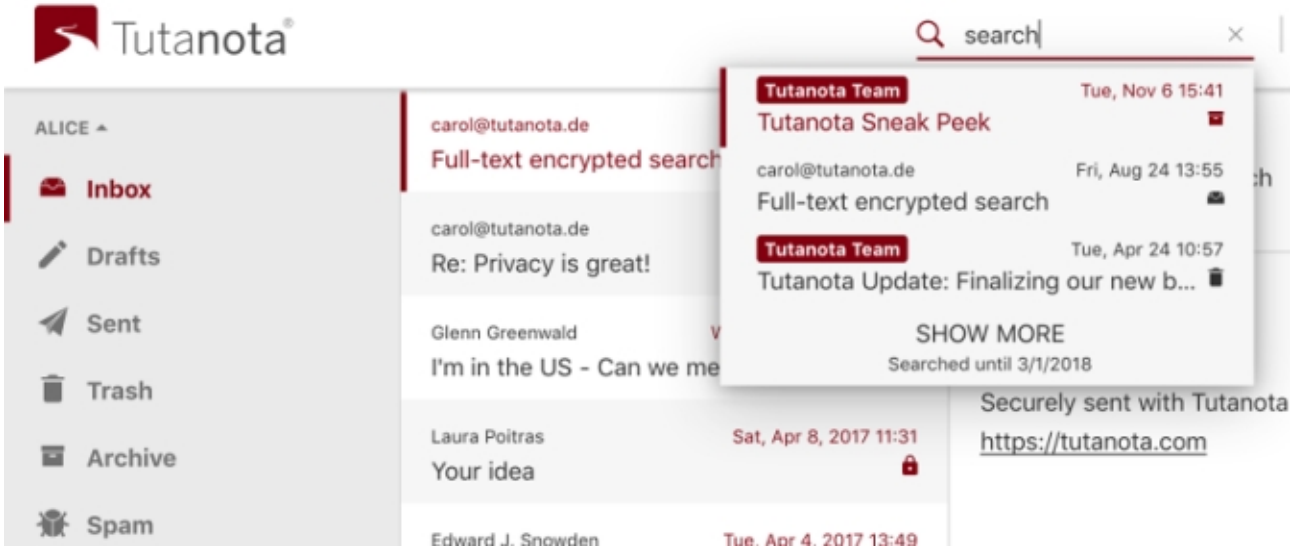


Mailfence is an excellent, free webmail service that not only encrypts your emails, but any calendars, notes, contacts, and documents you store using the service. All in all, for a free

service, Mailfence is up there with ProtonMail in bringing the power of encryption to anyone that would like to try.

MakeUseOf likes Mailfence for more than its excellent encryption and security offering. Mailfence owner and developer, ContactOffice, donates 15% of the income from their paid-for Pro plan to the Electronic Frontier Foundation and the European Digital Rights Foundation. Furthermore, Mailfence is based in Belgium, renowned for its strong privacy laws.

3. Tutanota



A Tutanota free account comes with 1GB storage and excellent end-to-end encryption. A premium account comes with extensive functionality, including sending Tutanota encrypted mail to non-Tutanota email addresses. (You can send encrypted mail to non-Tutanota email addresses with a free account, but you will have to arrange an alternative secure delivery method for the password to unlock the email.)

MakeUseOf's James Frew **reviews ProtonMail and Tutanota in his look at encrypted email providers**.

What is 2FA and How Do You Use It?

Two-factor authorization (2-FA) is an important additional email account security feature. 2FA is a process which requires you to enter two different passwords to unlock your account.

The first password is your unique password, as previously covered. The second verification password is usually a time-limited code that is sent to another device, although you can use a fingerprint or other biometric scan in its place. The idea is that only the legitimate account owner should have access to the second piece of verification data, drastically increasing security.

For instance, when I log into my email account, I enter my secure password. Because I have 2-FA turned on, moments later I receive a six digit code that I must enter into the login panel before the code expires. Without the second code, my email account remains locked.

You might have already encountered 2-FA when using an online banking portal, using a card reader or similar to create a one-time password to unlock your account. It isn't just your online banking that uses 2-FA—your email account can use it, too.

I don't have the space available to detail how to turn on 2-FA for the most popular services. **However**, I'm not leaving you hanging. Check out the following links to learn how to setup 2-FA:

- **How to Protect Your Apple Account Using 2-FA**
- The **EFF's short guide to using 2-FA with outlook.com**
- **Leo Laporte's Quick 2-FA Setup Guides**

Can You Stop Scammers Spoofing Your Email Address?

Last year, I received a surprising email. It was sent from my private email address back to the same address, and I was advertising some variety of dietary pills. From myself, to myself. A spammer was using my email address to send all kinds of irritating and potentially malicious mail. In a short time, my legitimate outgoing emails began heading straight into the recipient's spam box, filtered out because other people were (quite rightly) declaring my domain as a source of spam.

So, **can you stop spammers and scammers spoofing your domain**?

The answer comes down to your email provider. If you have control over the domain you send your email from, you can implement some of the measures in the linked article to stop a spoofer using your email address.

However, if you use a free email provider, such as Gmail or Yahoo Mail, you have less control over the additional security protocols your inbox uses. Don't take that the wrong way, though. Google and other free email providers still have a vested interest in stopping spam mail and email spoofing so using a free service doesn't automatically make you a bigger or easier spoof target than other services.

Email Security is Delicious

Email security is like a gigantic, delicious cake. To truly secure your email account, you need layers. A password, two-factor authentication, encryption, and a VPN are all vital layers in your email security plan.

Before reading the next chapter:

- **Follow** one of the 2-FA guides to secure your email account.
- **Check out** the free encrypted mail services and consider signing up for one.
- **Consider** how many layers your security cake has and if you could add more.

Chapter 5: How to Encrypt Your Emails

In this chapter you'll learn about encryption: encryption in Gmail and Outlook, considering third-party encryption utilities, and whether your emails need the additional security layer of encryption.

Encryption in Gmail

Google takes email security and privacy seriously. Well, to an extent. Remember, if you're not paying for the product, you are the product. (It isn't just you, there's billions of us!) However, for the most part, Gmail is a secure email service with enough functionality for the vast majority of users.

Gmail uses TLS encryption by default, so long as the recipient email server supports it. If you're sending email from and to a Google account, TLS is automatic. (TLS a basic-but-effective level of encryption that many email services will use by default—see our **article explaining email security protocols** for more information on TLS encryption.)

Only paid-for G Suite accounts can add a personal digital certificate to a Gmail account. (And even then, your workplace or G Suite administrator may turn off such functionality.) If you have a paid-for G Suite account, follow **Step 3: Upload Certificates** on the **official Google how to enable S/MIME tutorial**.

Otherwise, if you use a free Gmail account, feel free to skip forward to the **Third-Party Encryption Tools** section further down. It has some excellent third-party encryption tools that work perfectly with a Gmail account!

Encryption in Outlook

Like Gmail, Microsoft Outlook will use TLS encryption where possible (if the email server supports the encryption protocol).

Paid-for versions of Microsoft Outlook can upload a personal Digital Certificate to encrypt your email. That means those with an Office 365 subscription or with a standalone Microsoft Office license. Free versions of Microsoft Office Online and Outlook.com cannot install a personal digital certificate. This is a slight irritation, but nothing to worry about because there are secure third-party encryption tools—and you can check out three of the best down below.

Install Personal Digital Certificate in Outlook

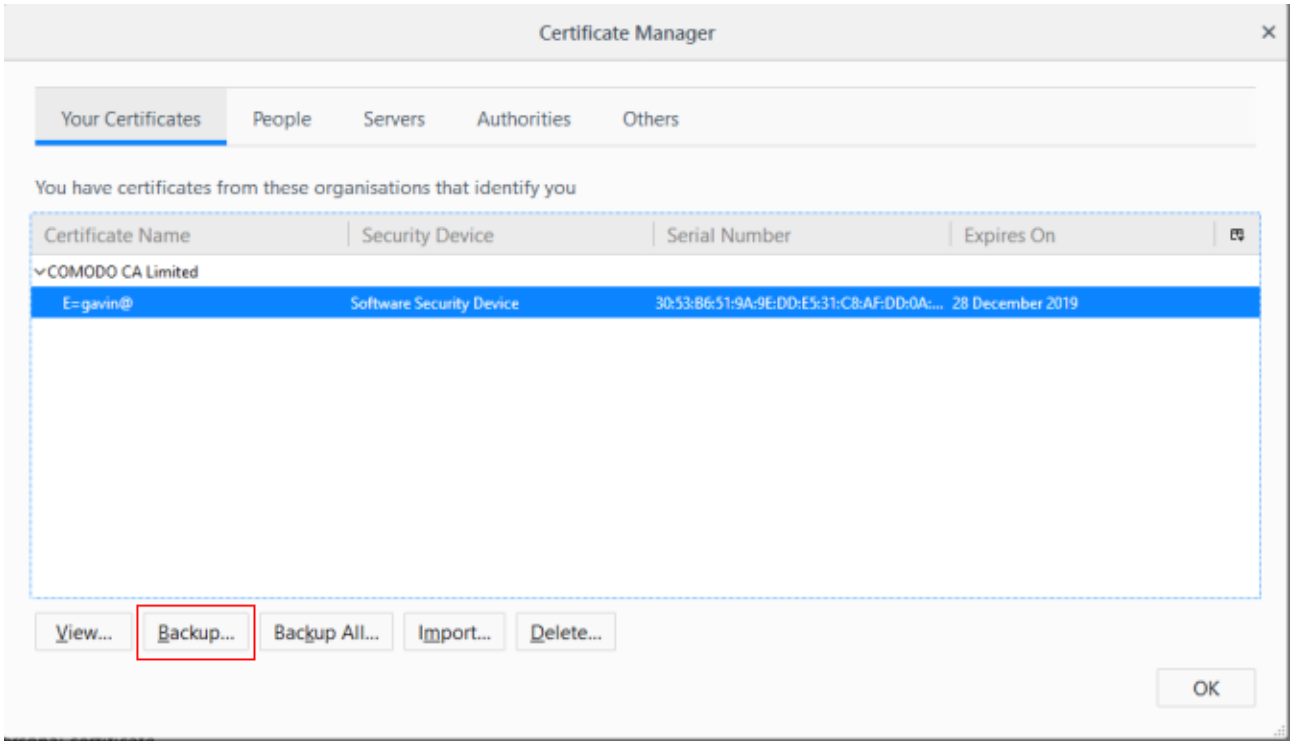
Here's how you install a personal Digital Certificate in Outlook. The Digital Certificate will allow you to sign and encrypt Outlook emails using S/MIME. However, your recipient must also support S/MIME, or the message will fail to send.

1. Using Mozilla Firefox, head to **Comodo's Install SSL** site. (You cannot use Microsoft Edge or Google Chrome for this task.)
2. Hit the large **GET NOW** button.
3. Enter the details for the email account you want to secure (that you use within Microsoft Outlook). Add a password. **Think back to the start of this guide** regarding password creation and strength. Accept the terms of the Subscriber Agreement and press **Next**, and follow the on-screen instructions.

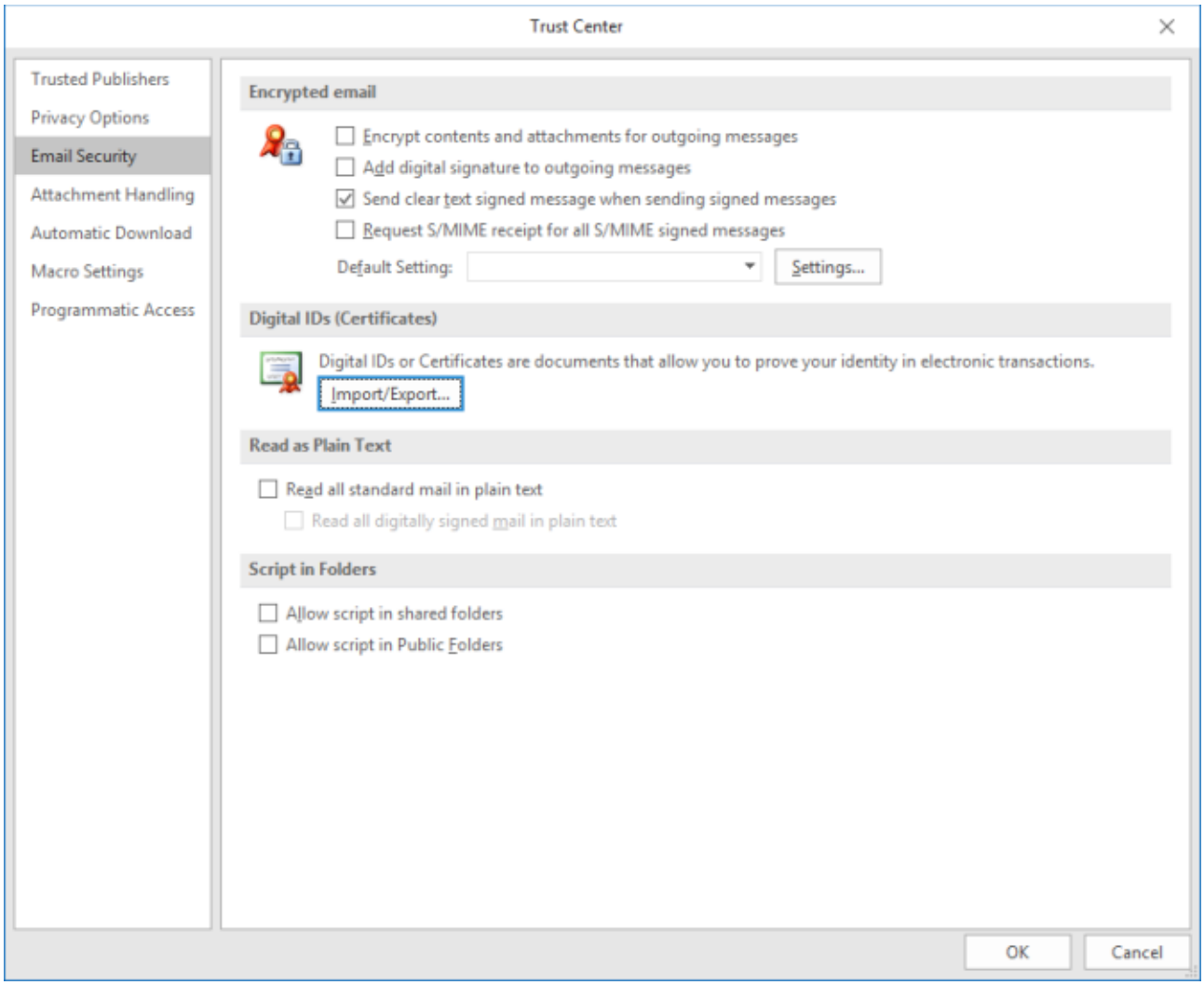
4. Head to your email account and open the Comodo collection email. Copy the link highlighted in the image below and paste it into the Mozilla Firefox address bar and press Enter. Enter your corresponding email address. Now, copy the **Collection Password** from the email into the Collection Password field and press Enter. Your Digital Certificate should immediately begin downloading (it will only take a second or two).

5. Next up, and still working within Mozilla Firefox, you need to extract the Digital Certificate from the browser Certificate Store. Reason being that the automatically downloaded certificate is in the wrong format. In Mozilla Firefox, head to **Menu > Options > Privacy & Security**, then scroll down to the Security section and select **View Certificates**.

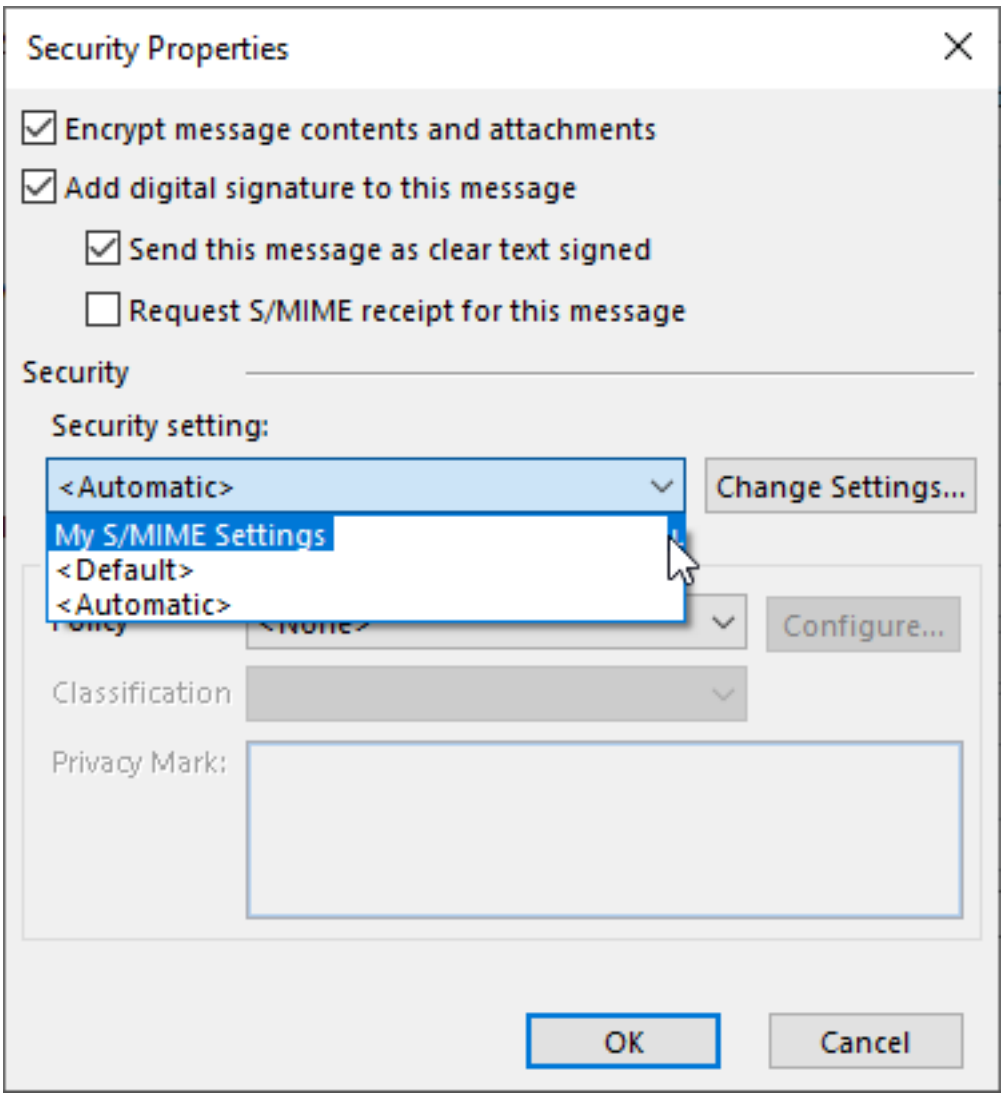
6. Select the **Your Certificates** tab, then select the Certificate Name for the relevant email address, and press **Backup**. Select a relevant and memorable filename, then **Save** the file to a memorable location. You must now create another password. **This password is very important**. It protects the backup file you are creating, as well as serving as a password when you install the Digital Certificate in another program.



7. Open Outlook. (I'm using Outlook 2016.) Head to **File > Options > Trust Center > Trust Center Settings > Email Security**. Under Digital IDs, select **Import/Export**, then browse to the location you saved the Digital Certificate backup, select it, then press **Open**. Now, **enter the backup password created in the previous step**, and continue with default settings.



8. Now, under the Encrypted Email section, you can add your **Default Setting**, using the **Settings** button to alter the level of encryption you add to each email.



As mentioned above, unless the person you are sending to also uses the same encryption protocol as you, your outgoing email will see an error message.

And that is frustrating. Unfortunately, if your recipient doesn't support incoming email encrypted with S/MIME, you will have to use an alternative secure messaging tool. For instance, the other email encryption methods listed below allow you to send an extremely secure message, to anyone, regardless of their inbox encryption settings.

Third-Party Encryption Tools

Encryption requires a password. The person you are sending an email to must have a way of unlocking your encryption. That is where public and private key cryptography comes to the fore.

Before continuing with this section on third-party encryption tools, **I strongly advise** you read section seven and eight of my article exploring **10 encryption terms you should know and understand**. It will make some of the upcoming information **much easier to digest**! Another extremely informative read is this look at **how encryption works and whether it is really safe**.

So, third-party encryption tools for email come in two shapes and sizes: for your desktop, and your browser. Desktop tools have the advantage of being multi-purpose, featuring Digital Certificate managers, decryption tools, and so on. Browser encryption tools have the advantage of being easy to use and normally have seamless integration with the service you are trying to use.

When should use your encryption? Sending an email to your friend about her delicious apple pie? You can send that without additional encryption. Sending an email to your friend containing banking information? You should encrypt that email. You **should encrypt emails containing sensitive information**. Traditionally sensitive information includes financial information, passwords, personally identifying information, and otherwise.

Here are three third-party encryption tools you should check out, as well as where you should use each tool.

1. OpenPGP

Okay, so OpenPGP is an open source encryption protocol that started life as Phil Zimmerman's groundbreaking PGP (that stands for Pretty Good Privacy—yes, that's the actual name) protocol. Zimmerman realized early on that the world needed a free, open-source encryption protocol and at the time of writing, thousands of applications around the world use OpenPGP.

There are several handy OpenPGP implementations for home users like you and me.

- **Windows:** Windows users should check out **Gpg4Win**
- **macOS:** macOS users should check out **GPGSuite**
- **Linux:** Linux users should check out **GnuPG**
- **Android:** Android users should check out **OpenKeychain**
- **iOS:** iOS users should check out **PGP Everywhere**

The implementation found in each of these programs is slightly different (they all have different developers putting the OpenPGP protocol to use encrypting your emails), but all are reliable. The key takeaway from these encryption tools is that you can freely encrypt emails to boost your security.

You can also email other users using OpenPGP standard tools, too. For instance, you could email someone using one of the upcoming webmail encryption browser tools straight from your OpenPGP enabled Outlook desktop client.

2. Mailvelope

Mailvelope is an easy to use browser extension for Google Chrome and Mozilla Firefox. Mailvelope combines the "advantages of a cloud-based webmail solution . . . with OpenPGP encryption."

It really is easy to use, working out of the box with webmail providers including Gmail, mail.ru, Outlook.com, Yahoo, Zoho Mail, and volny.cz. Furthermore, Mailvelope has help pages and support for GMX, Posteo, and WEB.DE.

3. FlowCrypt

FlowCrypt is another easy to use browser extension for Google Chrome and Mozilla Firefox that lets you encrypt your Gmail traffic, both emails and files in transit. There is a beta Android app still under development, and planned releases for macOS, iOS, and Linux, as well as client add-ons for Thunderbird and Microsoft Outlook.

FlowCrypt integrates seamlessly with Gmail. Many users point to the ease of setup and overall simplicity in comparison with other fully-featured encryption tools. However, unlike Mailvelope, FlowCrypt only works with Gmail accounts, so bear that in mind.

Encryption Is Easy

Encryption doesn't have to feel overwhelming. The OpenPGP desktop and mobile implementations may feel overwhelming to begin with. There are a huge number of online resources that can guide you through the installation, setup, and overall use of each tool to make sure your email remains secure at all times.

On the flip side, Mailvelope and FlowCrypt make sending encrypted emails to anyone simple.

Before reading the next chapter:

- **Check out** the free encrypted mail accounts, and consider signing up for one.
- **Think** about the third-party encryption tools and how they fit into your email routine.
- **Consider** which instant messaging apps you use and if you feel secure using them.

The final lesson is all about secure instant messaging tools: what are they, are they safe, and can they truly replace an email account? Give a thought to the instant messaging tools you use. Are you aware of their security features? Do you feel secure when you send a message?

Chapter 6: Are Instant Messaging Tools More Secure Than Email?

This chapter is dedicated to instant messaging services. What is an instant messenger? Can an instant messaging service replace your email account? And the key question: Are instant messaging services secure?

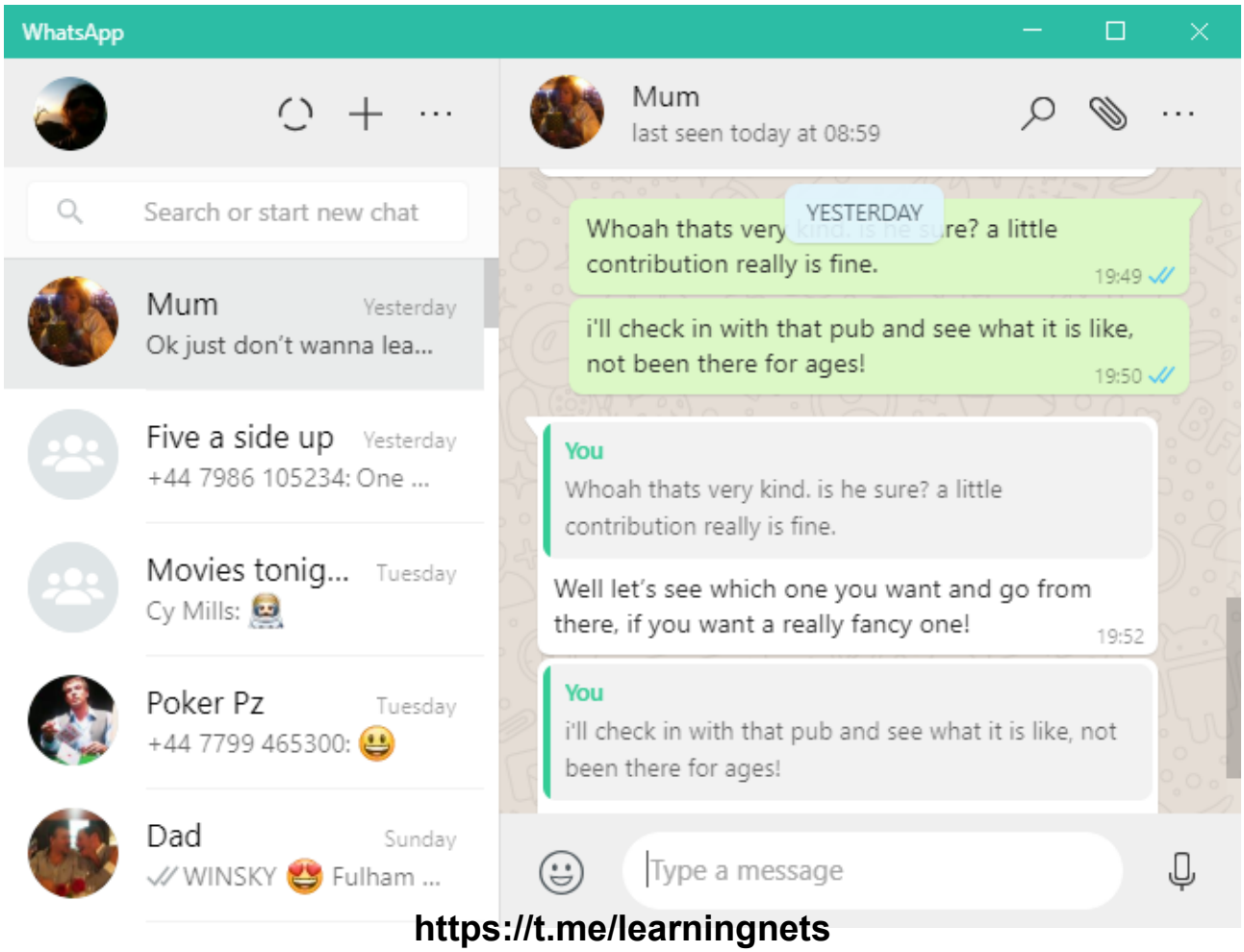
What Is an Instant Messenger?

An instant messenger is a service where you can send a direct message instantaneously to a contact. Contacts are usually friends, family, colleagues, and so on. Instant messengers have been an extremely popular method of communication since the early days of the internet, with modern instant messengers preceded by Internet Relay Chat (IRC), the Bulletin Board System (BBS), and other classic chat programs such as ICQ, MSN Messenger, AOL Instant Messenger, and others.

As for modern instant messengers? Think WhatsApp, Facebook Messenger, and other apps that let you ping a message straight to your friend. Depending on the service, you can send instant messages to and from your desktop, smartphone, tablet, and laptop.

Are Instant Messengers Secure?

There are several very secure instant messengers. One service, WhatsApp, is credited with **bringing end-to-end encryption (E2EE) to the masses**. With over 1 billion users, the Facebook-owned encrypted messenger provides an extremely simple method for people to shield their communication from prying eyes.



The fact that privacy destroying Facebook owns WhatsApp is beside the point, as the end-to-end encryption—that's encryption that protects your message from your device all the way to your recipients—is secure. WhatsApp uses the Signal Protocol, as does Facebook Messenger's Secret Conversation mode and more recently, Skype Private Conversations.

(Want to use Facebook Messenger Secret Conversation mode? MakeUseOf's Dave Parrack **shows you how to enable Secret Conversation mode**!)

Are instant messengers good to go then? Not quite. It really does depend on the platform.

- **WhatsApp**. Secured using the Signal Protocol, owned by Facebook. Also note that automatic backups to Google Drive renders E2EE useless as the service cannot encrypt the data once it leaves the service.
- **Signal**. The Signal Protocol developers, Open Whisper Systems, have a secure instant messenger called Signal (using the same secure protocol).
- **Telegram**. Secured using an encryption scheme called MTProto and is owned by Pavel Durov, the brother of the encryption protocol developer, Nikolai Durov. (The brothers also developed the Russian version of Facebook, VK.) The Telegram encryption receives regular criticism from encryption specialists for not being thoroughly tested as other encryption algorithms, yet the messaging service is still banned in Russia and attracts regular criticism from other governments.
- **Wickr**. Wickr is a popular E2EE messaging app that features the option for ephemeral messages—that is, self-destructing messages on a timer. In 2017, Wickr turned its encryption standard open-source, allowing anyone to make use of it and, most importantly, any security researcher or cryptologist to examine it for vulnerabilities fully. As it turns out, Wickr's end-to-end encryption is solid and will keep your messages safe.
- **Threema**. The Switzerland-based E2EE instant messenger bases its encryption on the open-source NaCl standard and has passed multiple external security audits to confirm the security on offer for your messages. Threema is the only app on this list with a small upfront cost, but for that small outlay, you get an extremely secure, featureful E2EE application.

How do you choose between the secure instant messaging apps? In my experience, that decision is down to the people you communicate with. Threema is an excellent secure app, but as none of my friends or family use it, I won't be using it either.

Want to understand more about online privacy and messaging security? Check out the MakeUseOf **guide to improving your online security and defending your privacy**. Alternatively, check out the MakeUseOf **guide to avoiding online surveillance as best as you can**.

Should You Use an E2EE Messenger Instead of Secure Email?

Deciding on the best method of secure conversation is difficult for everyday users and businesses alike. The level of security offered by the secure instant messengers is substantial. So substantial that numerous governments around the world want to ban their use. In countries with authoritarian regimes, such as Russia, Iran, and China, many secure messaging services are already banned and their use considered a crime against the government.

Alternatively, officials want the tech companies developing secure instant messengers to create encryption "backdoors" that would allow a government official to see the contents of a

secure message. The idea that a developer could create a single-use backdoor is fanciful and shows a considerable lack of understanding as to how encryption and secure messaging services work.

Check out this MakeUseOf article if you'd **like to understand why encryption backdoors are dangerous**.

The biggest difference between "regular" email encryption (e.g., TLS), an E2EE instant messenger, and email using advanced encryption (e.g., third-party encryption) is how the content of your message displays once received.

TLS encrypts your message content in transit, but once it hits your inbox, it displays in clear text where anyone can read it. It is a similar situation with a secure instant messenger. The message is secure with end-to-end encryption to protect from prying eyes in transit, but once it arrives on your device, be that laptop, smartphone, or otherwise, the message will display in cleartext.

It is here that certain third-party encryption tools hold a significant advantage over the alternatives. Once a message hits your inbox, depending on the encryption utility you use, it will not automatically display the contents until manually decrypted.

So, to answer the question, secure instant messengers are a fantastic, easy access utility that provides secure communication for billions of people every day, without having to give encryption, keys, passwords, and privacy much thought. But to replace secure email? Instant messengers have some way to go.

Just to be clear:

- E2EE instant messages are excellent. You can use an E2EE message on a messaging app to send any message encrypted in transit. However,
- An email secured using encryption is theoretically more secure than an E2EE message because of the additional layers of security you can add.

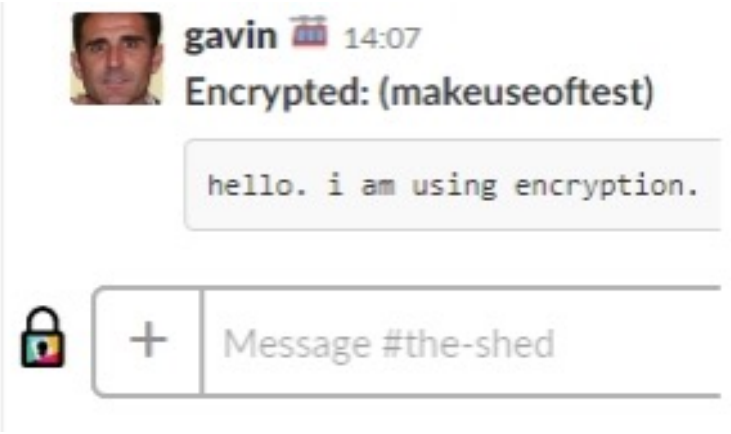
What About Slack?

Slack is a messaging service for organizations. Each team member has an account and can send a message to the rest of the users. Slack has been a revelation amongst messaging services, offering enormous workplaces the opportunity to run a private internal messaging service. It isn't only for massive workplaces, though. My friends and I use a private Slack channel to keep in touch, for instance.

The big question for many Slack users is "are my messages secure?" Unfortunately, the answer is simple: They are not as secure as you would hope. In that, paid-for Slack chat administrators can access and download the entire Slack chat history, including private chats. If an administrator turns this feature on after the Slack channel is open, users will receive a message informing them, but there is little a user can do other than rapidly delete messages that must remain secure.

I wrote previously about **how to use encryption tools with Slack, including the Shhhlack add-on**. The add-on itself is very easy to use and does increase the security of Slack users, but not every user will want to make the additional effort. Furthermore, some workplaces will find the use of a third-party Slack encryption tool a direct offence and you could be on the receiving end of a caution, or worse.

Here's what an encrypted WhatsApp message looks like to the sender:



Bringing E2EE to the Masses

There's no doubt that WhatsApp has a strong shout as the tool that truly brought easy end-to-end encryption to the masses. Whether every user understands the power of E2EE, or would even care if they did realize is another question. The most important thing is that the option for encryption is there for the moment people want to send a secure message.

Do you use a messaging service? Will you now switch to a more secure service? And would you ever consider leaving email behind completely if an instant messaging tool could offer the same functionality?

Before reading the next chapter:

- **Check out** the other secure instant messenger services.
- **Read** about **why encryption backdoors are a terrible idea** and why encryption is extremely important.

Chapter 7: The MakeUseOf Email Security Roundup

You're now reaching the end of this guide. Hopefully you've learned a lot about securing your inbox, protecting your incoming and outgoing mail, and making sure you are the master of your own (email) domain. So, why is there another email appearing in your inbox?

I thought a quick email security guide run-down would make the perfect end to a week where you have drastically increased the security of your inbox.

Chapter 1: Why Do You Need Secure Email?

In Chapter 1 you learned about the reasons behind secure email; why security is important, what it helps, and what a secure inbox stops taking place. You also took a look at the value of encryption and why your inbox, as well as the rest of the internet, cannot do without it. The final piece of information in this chapter was also one of the most important: email isn't secure.

Here is the most important link for you to follow up from Chapter 1:

- **7 email security protocols explained**

Chapter 2: Do You Make These Common Email Security Mistakes?

Chapter 2 covered the most common email security mistakes that everyone makes. Mistakes such as clicking suspicious links, reusing weak passwords, and poor spam filtering exposing your inbox to malicious email. You also learned the five best ways to spot spam and scam emails, as well as how to turn up your spam filter to reject more of the nasty stuff trying to get in. Finally, you took a long hard look at your passwords and whether they're a critical issue in your email security.

Here are the most important links for you to follow up from Chapter 2:

- **Tips on spotting malicious phishing emails in your inbox**
- **How to tweak your Gmail junk email filters**
- **How to tweak your Outlook junk email filters**
- **The MakeUseOf guide to choosing a password manager**

Chapter 3: How to Use Your Email Account Securely

This was a short lesson in using your email account securely. You looked at six tips that will secure your email account access in almost any situation. Furthermore, you learned about stopping scammers spoofing your email address as well as how you add two-factor authentication to your email account.

Here are the most important links for you to follow up from Chapter 3:

- **5 excellent reasons to consider upgrading to Malwarebytes Premium**
- **The reasons why a paid-for VPN always trumps a free alternative**

- **The best unlimited free VPNs you can get your hands on**
- **The MakeUseOf guide to the best paid-for and free VPNs**
- **What to do before every Windows Update hit your system**

Chapter 4: How to Choose a Secure Email Provider

In Chapter 4, you were figuring out what features to look for in a secure email provider. There were also a handful of suggestions regarding secure email services, some free and some paid-for. In Chapter 4, you also learned how to use your email account securely, looking at both desktop and mobile security tips.

Here are the most important links for you to follow up from Chapter 4:

- **Is Gmail or ProtonMail better for your email account requirements**
- **Reviews and comparisons of ProtonMail and Tutanota**
- **How to Protect Your Apple Account Using 2-FA**
- The **EFF's short guide to using 2-FA with outlook.com**
- **Leo Laporte's Quick 2-FA Setup Guides**
- **Can you stop spammers and scammers spoofing your domain?**

Chapter 5: How to Encrypt Your Emails

In Chapter 5's email security lessons, you learned about email encryption: third-party tools, how to encrypt emails in Gmail and Outlook, and the pros and cons of using additional encryption to secure your email.

Here are the most important links for you to follow up from Chapter 5:

- **10 encryption terms you should know and understand**
- **How encryption works and whether it is safe?**
- **7 email security protocols explained**
- **5 common encryption algorithms explained**
- **Don't believe these 5 myths about encryption**

Chapter 6: Are Instant Messaging Tools More Secure Than Email?

Instant messaging apps play a huge part in our day-to-day communication, so why not consider their security and privacy on the same level as your email account? That's what Chapter 6 was all about: are instant messaging apps secure? Moreover, are they secure enough to replace your email account entirely? There were some handy tips on which instant messaging apps are the most secure.

Here are the most important links for you to follow up from Chapter 6:

- **Why WhatsApp end-to-end encryption is a big deal**

- How to enable Facebook Secret Conversation mode
- The MakeUseOf guide to online security and privacy
- The MakeUseOf guide to avoiding online surveillance
- Why encryption backdoors are extremely dangerous
- How to use encryption tools with Slack

Course Complete: Your Email Is Secure

Okay, you have now worked your way through the MakeUseOf email security course!

You now carry the powerful knowledge of how to keep spammers, scammers, and other ne'er do wells out of your inbox. You know how to scramble the contents of your outgoing emails so only the recipient can read them. There was information on secure email providers, third-party encryption tools, and even tips on how to securely access your email from any device.

Thank you for reading and learning.