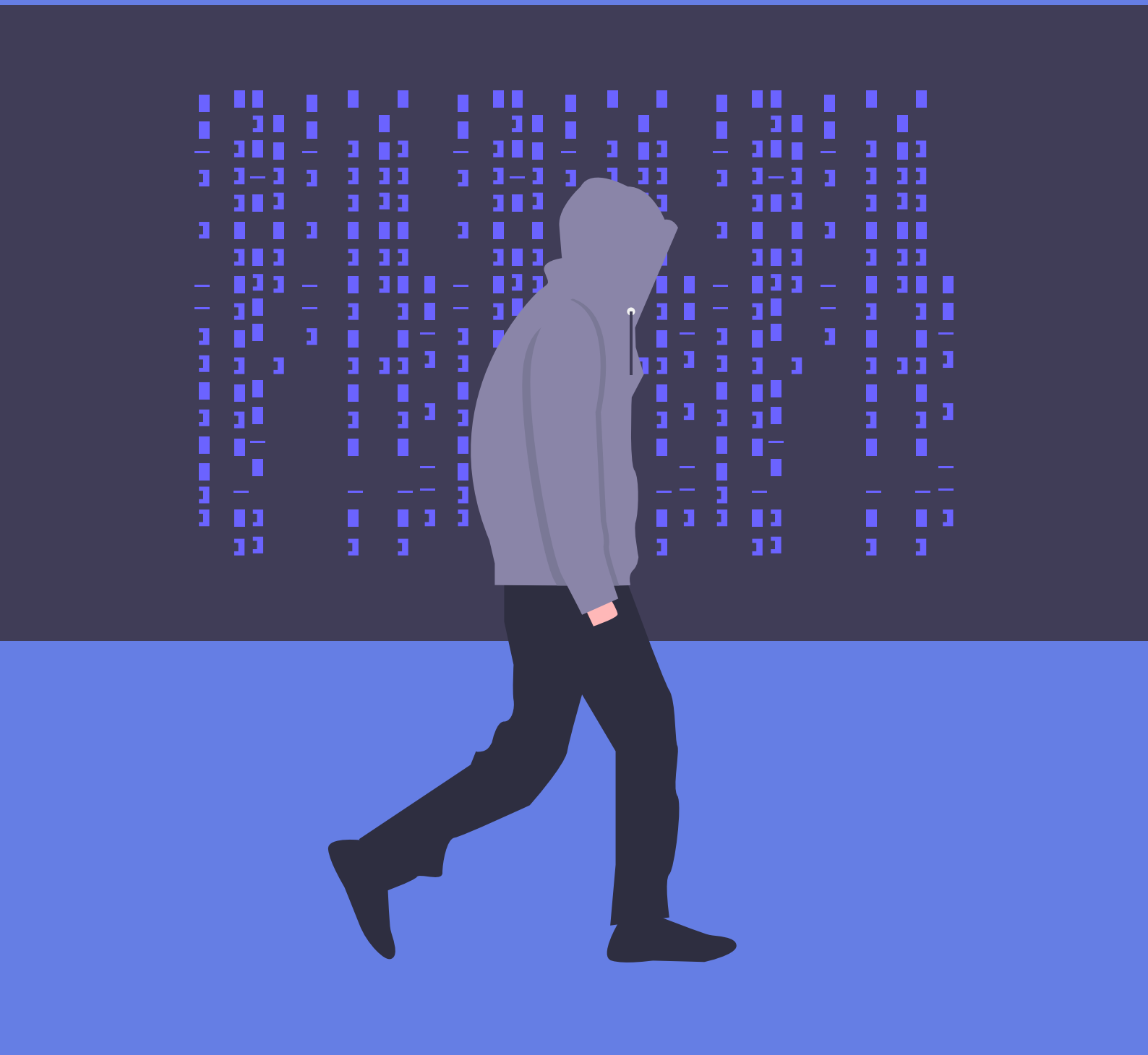
The ProtonMail Guide to IT Security

for Small Businesses

The ProtonMail IT security team



Introduction

How to use this ebook

READ THIS EBOOK to understand the basic steps you can take to help your business improve its IT security

This ebook aims to help you understand the concrete steps you can take to improve the IT security of your company. ProtonMail has been a leader and innovator in secure communications since we first launched in 2014. Thinking through how to address the various security and privacy problems one faces when creating an end-to-end encrypted email service has given us unique insight into IT security, and we want to share that insight with you.

So, what exactly do we mean by IT security? Information technology security, or computer security, or cybersecurity, is a set of strategies and policies meant to protect an organization's IT landscape, including devices, software, and electronic data, from unauthorized access or damage. The purpose of IT security is to maintain the integrity and confidentiality of your company's sensitive information and to prevent the disruption of your company's services.

Yes, IT security can be very technical and expensive, but it does not have to be. Many of the steps we discuss in this ebook are fairly simple and do not require a massive budget. In fact, many of the most important steps you can take to reduce the risks of a data breach are free.

We have tried to make this ebook as practical as possible by giving you concrete steps, designating who should be in charge of what processes, and ending each chapter with an easy-to-follow list of best practises. **As such, you do not need to read this entire ebook cover to cover. Each chapter was written to stand on its own,** although there may be references to previous chapters. Think of it as more of an IT security guide than a textbook.

Note that this guide is not exhaustive, nor will it cover all the needs of every company. However, **we will cover the fundamental IT security best practices, processes, and tools that all companies should apply.**

This ebook's intended audience

While this ebook contains IT security tips that everyone can use, it will be the most helpful if:

1. Your business uses computers or other Internet-connected devices and handles sensitive data.
2. You are the single decision maker or one of the decision makers for a small or medium-sized business IT security.
3. You are not an IT security expert, but you do have a basic understanding of technology and some IT tools. For example, you know what a VPN is and what it is used for.
4. You are looking to improve your IT security, but you are not sure how and you want to determine what you can do internally before bringing in an IT security consultant.
5. Your company does not run its own internal network, but you may consider establishing one in the future

How this book is organized

Each chapter in this ebook covers a specific subsection of IT security. All chapters, except for Chapter 5, end with a checklist or list of best practices that the targeted audience can use to ensure they are following IT security best practices. Again, feel free to jump directly to the chapter that you think will be most useful for you.

Chapter 1

Prepare your IT security framework

This chapter introduces you to the basics by defining what IT security means and what you should do to start the process of securing your business's data .
It ends with a checklist for you, the primary decision maker for your small business.

Chapter 2

Create a culture of IT security awareness

Your employees will make or break your company's IT security. This chapter discusses the best practices that you should train your employees to use daily. It ends with a list of best practices that your employees can review to make sure that they are not compromising your company's data.

Chapter 3

Enforce email security

Email is the most common method used by attackers to get sensitive information or deliver malware onto a device or network. This chapter explains what steps your employees can take to avoid becoming the victim of phishing emails. It ends with a list of best practices for your employees, describing what they should do when they receive an email that they were not expecting.

Chapter 4

Protect your network

Network security is the process of making sure that no unauthorized parties can access or abuse your devices or data. This is a more technical chapter, for businesses that are growing and thinking about creating their own internal network. It ends with a list of best pratices for your IT security leader, explaining the basic steps they can take to maintain security in a small business and some of the more advanced steps they can take to establish and maintain a secure internal network.

Chapter 5

Adopt top IT security solutions for small businesses

This chapter is a list of all types of tools, programs, apps, and services that small businesses can use to improve their IT security.

Chapter 1:

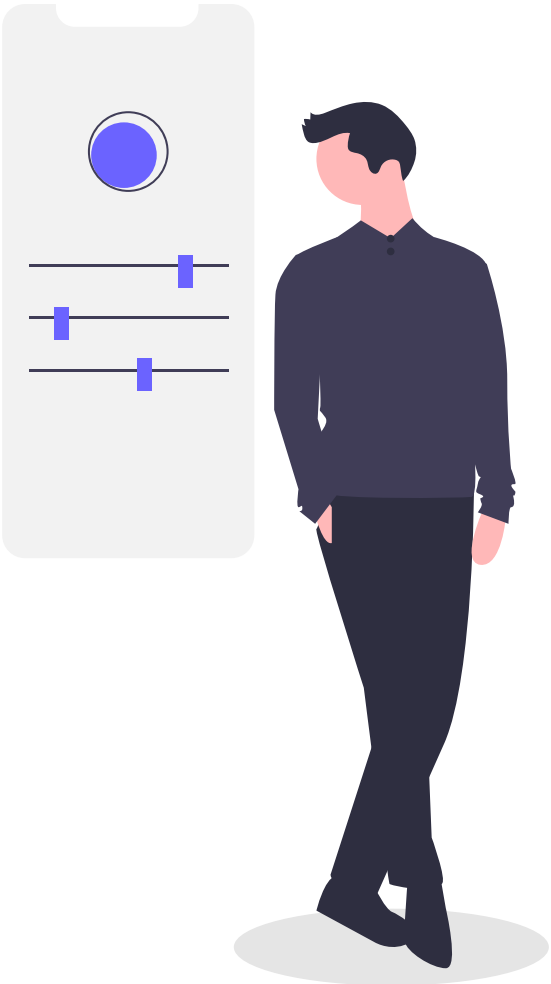
Prepare your IT security framework

READ THIS CHAPTER to see what steps you should take to begin the process of improving your company's IT security, including:

- Designate an IT security leader
- Create a threat model
- Formulate company IT security policies
- Business owner's IT security framework checklist

IT security can be a thankless job. It is difficult, requires constant vigilance, and when done correctly, it is almost invisible. People generally only think about IT security after there has been a failure, like a hack, a breach, or a data leak. Unfortunately, by this point, it is already too late.

Many small business leaders understand that IT security is important in theory, but feel that their company is so small that they will never be targeted. This is a mistake. Even if the majority of data breaches in the news involve massive corporations, studies have found that most of the victims of data breaches are small businesses.

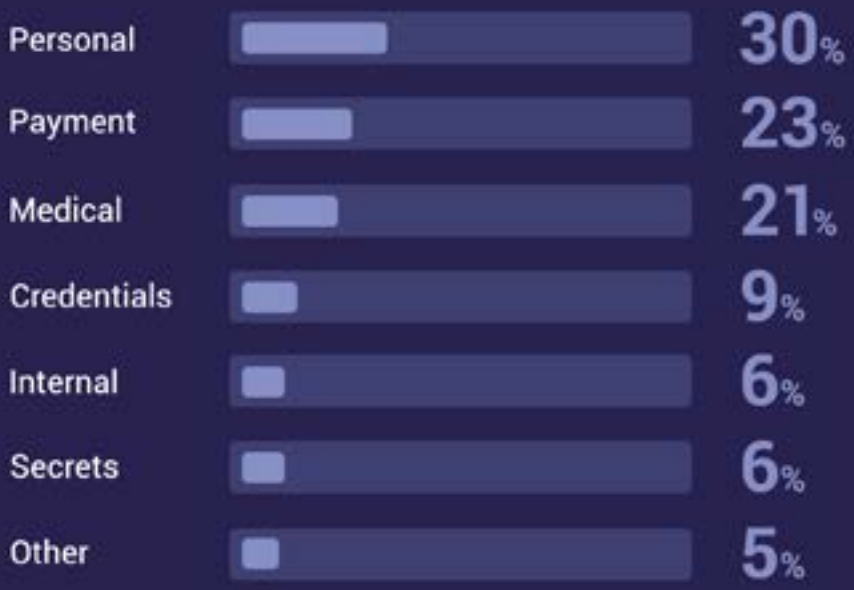


Think your company is too small to be targeted by hackers?

58% of the victims of data breaches are small businesses.

Small business, BIG TARGET

Types of data exposed in data breaches



74%

of small businesses feel they are not "well prepared" for a cyberattack on their company.

Reasons for weak cybersecurity

57% Lack of budget

54% Lack of time

37% Insufficient staff training

Yet the effects of a cyberattack can be severe

53% midmarket companies said cyberattacks resulted in financial damages of more than $500,000.

38% said they cost over $1 million.

As the decision maker for your small company, you set the tone. If you prioritize IT security, so will your employees. You must factor IT security into all of the decisions you make, from hiring personnel to how you lay out your office. To show that IT security is a priority, you should treat it like you would any area of your business; assign it a manager. Once you have an IT security leader, you need to work with this person to carefully assess the sensitivity of your company's information and your company's potential IT vulnerabilities. Once this assessment is complete, you then must create policies that describe how to secure that information and what to do if there is a data breach — having these plans in place makes determining which actions to take more straightforward, especially in times of crisis, like after a data breach.

Designate an IT security leader

IT security requires constant diligence, like following up with employees to make sure they are following all the IT security best practices. This is likely a task you will want to delegate to an official IT security leader. Depending on the size of your business, this person could be from your IT team (if you have one), but not necessarily. Initially, their experience with technology will matter less than their willingness to learn about IT security and hold team members accountable for completing training sessions and implementing digital safety practices.

Your IT security leader will be in charge of the day-to-day responsibilities of maintaining your company's IT security. It is important to note that as your business grows, so will the demands on your IT security leader's time and technical expertise. Eventually, this side task will become a full-time, salaried position.

Here are the five main responsibilities that your IT security leader should be in charge of:

Training and updating employees on IT security

The first step is training. Training sessions should happen soon after a new employee starts and then be updated periodically. The training should emphasize the most important aspects of your IT security policy while also giving employees an understanding of the specific threats your management team has identified. These should be specific to your organization and your industry. For example, if there are known threats targeting companies similar to yours through particular attack vectors, these training sessions are an excellent opportunity to educate your staff about preventing such attacks.

Some teams or individuals may be more vulnerable to attack than others based on their specialty or level of access. Network administrators, managers, and anyone handling payroll or customer data may need additional training and attention.

Your IT security leader should also regularly monitor the news and tech blogs. New vulnerabilities and attack vectors are being discovered all the time. They should inform

your employees of any relevant new or trending attacks and compromised services immediately.

Supplying employees with the proper tools

IT security requires that specific tools and programs be used, depending on what tasks the employee does and your threat model. Specific tools are necessary to address particular situations. For example, employees who regularly work remotely should use a reliable VPN service to protect their online activity. We outline the tools required to secure personal devices in Chapter 2, your business email in Chapter 3, and your business's network in Chapter 4, but it is the responsibility of your IT security leader to ensure your employees have access to the proper tools.

Assessing employees' knowledge of IT security

IT security never stops; there is still work to be done, even after employees have been trained and been given the proper tools. Your IT security leader should regularly evaluate your employees on their implementation of the IT security and email security best practices list. (See Chapters 2 and 3) This could be as simple as periodically sending out a test to employees to see if they can correctly identify potential phishing emails (see Chapter 3) or having a monthly, one-on-one chat with employees to ask them how well they implemented the best practices list.

Maintaining network security

This is the portion of the IT security leader's duties that will grow the most dramatically as your business grows. Once you install your own private servers and create an internal network, maintaining your networks' security will take up a large portion of the IT security leader's time. See Chapter 4 for the IT security leader's basic and advanced best practices list.

Consulting on IT security issues and carrying out IT security policies

Any time your company is making a major IT security decision, your IT security leader should be the point person leading the discussion. This includes evaluating different vendors and giving an informed opinion on future tech policies.

In the case of an emergency, like a data breach or unauthorized access to a company device, the IT security leader should take charge of implementing the relevant IT security policy.

Once you have your IT security leader, you can proceed to the next step.

Create a threat model

A threat model is a method of identifying and evaluating the security and privacy risks your company faces to mitigate them. It is the first step any company must take to determine its IT security priorities.

When creating your threat model, you should consult your IT security leader and any senior technology officers in your company. When creating a basic threat model, you should consider how the following three factors apply to your company:

Assets

Employee data, client credit cards, trade secrets, money, etc. List the things of value your company holds, where and how they're stored, and who has access to them currently.

Threats

Hackers, disgruntled employees, competitors, cybercriminals, governments, etc. Be as inclusive and imaginative as possible. You'll rank these threats later when assessing risks.

Potential vulnerabilities

Human error, unsecured communications, poor network security, unencrypted service providers, etc. Your past experiences, knowledge of your own systems, and existing research about data breaches can help you here.

At this point, it will probably be helpful to create a data flow diagram. These diagrams allow you to more clearly visualize the process your team uses to collect and process data. It also allows you to see which systems and employees you are trusting with your data. Once you have a full understanding of how data moves through your company and who controls that data, you are ready to consider the next two factors:

Risks

Which teams are most susceptible to threats? Which assets are most valuable? This analysis will help you decide where to focus the most energy.

Countermeasures

IT security awareness training, end-to-end encryption, access controls, data minimization, etc. Based on the information you've already compiled above, you can determine how to mitigate risk.

By the end of your threat model, you should know which data is most sensitive, what portion of your network or business you should focus on most to secure, and which employees will be critical to this effort.

For an example of a data flow diagram and a more thorough guide to threat modeling, click here.

3 Formulate company IT security policies

Now that you have identified which data are most valuable and what threats they face, you are ready to create your IT security policies. Again, this should be done with input from your IT security leader and any other senior technology officers in your company.

Some of your employees might complain that IT security measures add extra steps to previously simple processes. While this is not always the case, it is undeniable that, occasionally, increased security can lead to a trade-off with convenience. Your policy should attempt to maximize the gains in IT security while minimizing the inconvenience.

Receiving a copy of your IT security policy should be a part of every employee's onboarding, and your IT security leaders should regularly refer to this document and issue periodic reminders of its contents. It is not just another boilerplate HR document. Understanding your IT security policy and following it is part of everyone's job.

IT security policy

Your business's IT security policy should include basic guidelines that all employees must follow as well as broader principles that your business upholds. The lists of best practices at the end of Chapters 2, 3, and 4 are good examples of basic guidelines that your company can use as the starting template of its IT security policy.

As far as higher principles, these will vary depending on your industry, but the following three will apply to most companies.

Only collect personal data you need

The more information you collect, the more you must secure. If the data is not absolutely necessary for your service or product, you are better off not collecting it in the first place. If you operate a website, do you really need your readers' telephone numbers for their account? Probably not.

Only keep data for as long as your legitimate business allows

There are often laws that require data to be discarded once a transaction is complete. Similar to the first principle, the longer you keep data that is no longer necessary for your service, the more data you will have to protect. While you will need to set up a process to securely dispose of unnecessary data, this is still a better security option than holding on to those records indefinitely.

Apply data security principles to hard copies of data

This guide focuses on maintaining your company's secure control of its devices, networks, and electronic data, but it is important to remember that many companies have a large amount of data available as paper files. These files should also be considered as your company puts together its security policies.

Data breach policy

In an ideal world, you will never use your data breach policy. But if you ever do face a data breach, you will be relieved that you have already laid out the steps you need to follow. This policy does not need to be shared with all employees; only members of your IT security team and senior management need to be aware of it.

Secure data

Once you detect a data breach, your priority must be to find the cause and shut it down. You want to stop the current data leak and prevent any additional data loss. Once the breach has been contained, you should try to understand who was responsible and how the breach occurred (for this kind of technical analysis you will likely need to hire outside expert help). Also, see if you can track where the data went. If you see it exposed on another website, you should write to have them take it down. Finally, interview the people who found the breach and document every step you took to resolve the problem. These documents will help customer service respond to questions and will be useful in the future when evaluating security risks and breakdowns.

Fix vulnerability

Once the data breach has been stopped, you need to put in place additional safeguards to prevent future failures. This step cannot be done until you have located the cause of the breach. If the breach involved a service provided by a third party or a vendor, you should seriously consider what your other options are going forward.

Notify authorities and those affected

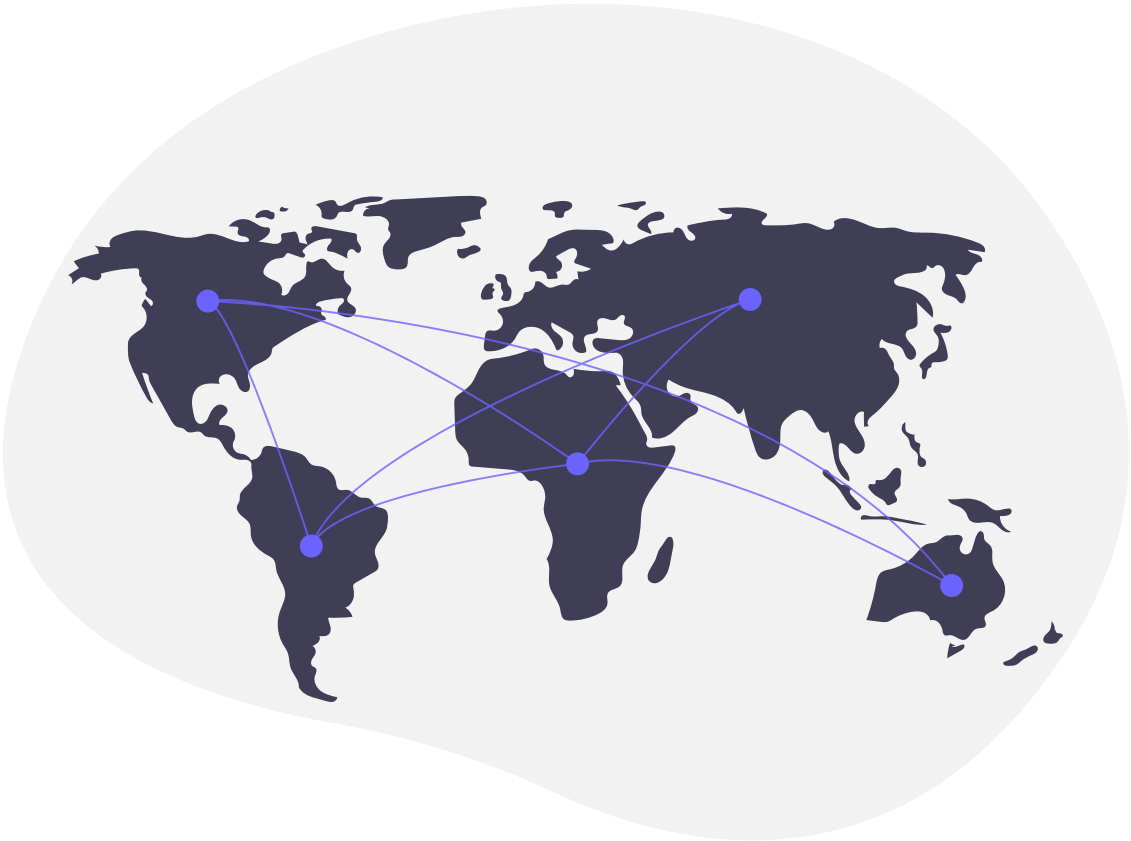
Finally, you must prepare a statement describing what happened as soon as the full extent of the breach is known. You should communicate with all the affected parties — including your customers, your employees, your investors, business partners, and any other stakeholders. Your statement should not contain any misleading information or withhold any pertinent details.

In many jurisdictions, there may also be legal requirements to alert either the businesses or customers directly affected. You should contact the relevant authorities and offer your full cooperation in resolving the issue.

Business owner's IT security framework checklist

Security best practice	Status*
Designate an IT security leader	
Create a threat model	
Formulate an IT security policy	
Formulate a data breach response policy	
Train your employees	
Regularly run security awareness programs	

*Tick if completed



Chapter 2

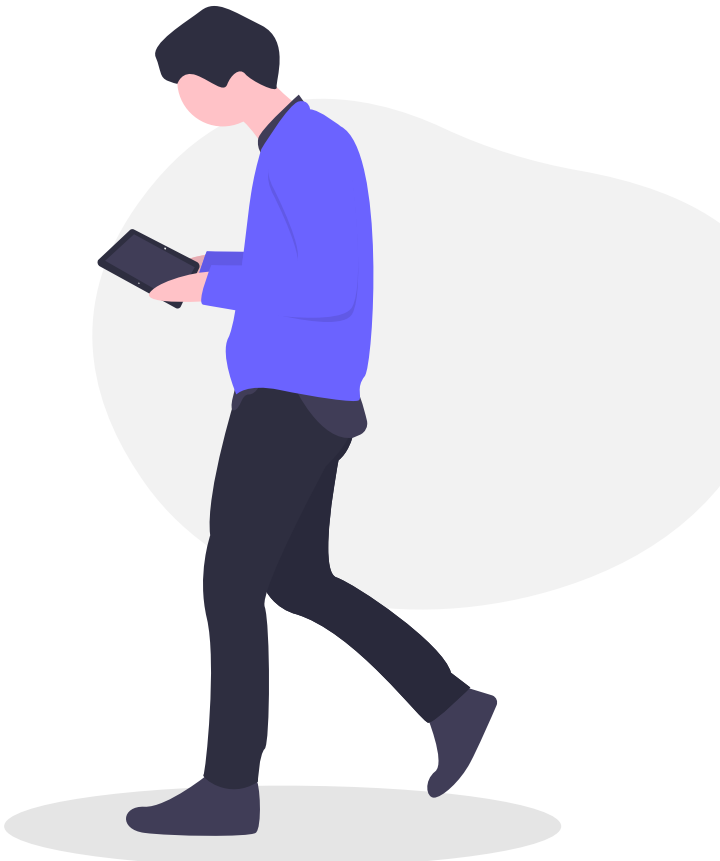
Create a culture of IT security

READ THIS CHAPTER to identify the IT security best practices for:

- Laptops and computers
- Smartphones
- Passwords
- USBs
- Employee IT security best practices list

Small business IT security is often overlooked, either due to a lack of expertise or funding. This is a mistake. Data breaches are costly to mitigate but potentially more costly to recover from after they occur. But not all data breaches are the result of a malicious attack by a hacker. Statistically speaking, there is someone that is an even bigger risk to your data than a hacker: your employees.

At least until the robots take over, your business will employ and rely on other human beings. They can be your best defense against cyberattacks — or your most significant vulnerability. Training your staff on basic IT security practices is a good start, but it is not enough. You must emphasize the importance of IT security and turn it into part of the office culture so that employees do not think of IT security as a one-off task, but rather as part of their daily routine. This chapter will help you identify the necessary steps that your employees should all implement.



Humans are the **WEAKEST LINK**

Employees are your company's biggest asset, but they can also be a hacker's key to your company's confidential information.

It only takes one victim

96% Email remains the favorite channel for hackers, with **96%** of all phishing and social engineering

Small organizations

In **2018**, employees of small organizations were more likely to face email security threats — including spam, phishing, and emailed malware — than those in large organizations.

Will your team spot the threat?

Ransomware is also a significant concern. According to the Ponemon Institute, more than **4,000** ransomware attacks occur every day in the US alone.

Cybersecurity experts reported that most ransomware programs are unleashed after employees fall for phishing or social engineering attacks.

How was the ransomware unleashed?

- **43%** Phishing/social engineering
- **30%** Insecure/ spoofed website
- **15%** Malvertisements
- **8%** Social media
- **4%** Other

Malicious email rate by organization size

Organization size	Malicious email rate
1-250	1 in 323
251-500	1 in 356
501-1000	1 in 391
1001-1500	1 in 823
1501-2500	1 in 440
2501+	1 in 556

IT security: neither impossible nor impractical

When people hear the words "IT security" their eyes often glaze over: they assume it is an impossibly technical subject and, therefore, too complicated for them to understand or have any impact on. While explaining how a TLS handshake works is very complicated, that level of knowledge is not necessary. **You can profoundly improve your IT security through relatively simple behavior changes.**

The measures you put in place will depend on the **Threat Model** (see Chapter 1) you developed. The important thing is that these IT security choices are made after a deliberative process in which the risks and rewards are weighed. While the following steps represent basic best practices, not every step will be appropriate for every business.

With that caveat out of the way, let's jump into measures you should take to secure your company's data.

Your IT security leader

As part of devising your IT security policy, you designated an IT security leader (see Chapter 1) to train your employees on IT security best practices and ensure those practices are regularly implemented. Your IT security leader must also be prepared to answer any questions your employees may have about how to protect their devices or the data they work with.

It is this individual's responsibility (with your support, of course) to cultivate a culture of IT security in your office. To create a culture of IT security awareness and keep best practices at the front of your employees' minds, your IT security officer will need to assess their IT security performance regularly.

Laptops and computers

If your business works with data, most likely that means that your employees either work on computers you supply or use their own laptops. In either case, making sure these devices are secure is vital to your overall **Network Security** (see Chapter 4).

Keep your operating system and software up-to-date

New security flaws are discovered in software every day, which companies fix in the updates they release. However, if you do not actually install the updates, then your device is not secured against these known threats, making it a tempting target. The best solution is to set your device to update automatically.

Windows

For Windows devices: In Windows 10, all updates are done automatically. Press **Windows Key + C** and select Settings. Once the Settings window opens, select **Update & Security**. This

will automatically take you to the Windows Update page. Here, you can see whether you have any updates pending. By clicking **Change active hours**, you can set the times for when your device will attempt to update itself.

Apple

For macOS devices: In macOS 10.6 and later, go to Apple Menu and click **System Preferences**.... Once the System Preferences window opens, click **Software Update**. Once the Software Update window opens, click the box next to Download important updates automatically (for Mac OS 10.7 users, this will read Download updates automatically). From the Check for updates: drop-down menu, you can choose how often you would like to check for updates. We recommend you pick **Daily**.

Enable a local firewall to block incoming network connections

A firewall examines traffic from your network (see Chapter 4) or the Internet, determines what is good traffic, and lets it pass while blocking all the rest. Enabling the firewall on your device prevents intruders from getting unauthorized access to your device.

Windows

For Windows devices: In Windows 10 and later, press **Windows Key + C** and select Settings. Once the Settings window opens, select **Update & Security**. This will automatically take you to the Windows Update page. Click **Windows Security**. Once the Windows Security window opens, click **Open Windows Defender Security Center**. A new window will open. Click **Firewall & Network Protection**. Here, you can see whether the firewalls for your domain, private, and public network are on.

Apple

For macOS devices: In macOS 10.6 and later, go to **Apple Menu** and click **System Preferences**.... Once the System Preferences window opens, click **Security & Privacy**. Once the Security & Privacy window opens, click on the **Firewall** tab. Then, click on the lock icon in the bottom left corner of the window. You will need to enter your administrator password. Click Turn On **Firewall**.

Enable full disk encryption

Full disk encryption applies encryption to your entire hard drive. This protects your files, pictures, software, and programs from being accessed if your device is stolen or lost.

Windows

For Windows devices: Some **Windows** devices automatically encrypt your disk, others don't, which makes it complicated. To check on Windows 10 and later, press **Windows Key + C** and select **Settings**. Once the Settings window opens, **select System**. Once the System window opens, select the **About tab**. In the About window, scroll to the bottom. If your device enables full

disk encryption, you will see an option to turn off Device Encryption. If you do not see it, you will need to download Veracrypt, which will encrypt your Windows 10 PC's system partition for free.

Apple

For macOS devices: In macOS 10.6 and later, go to **Apple Menu** and click **System Preferences**.... Once the System Preferences window opens, click **Security & Privacy**. Once the Security & Privacy window opens, click on the **FileVault** tab. Then, click on the lock icon in the bottom left corner of the window. You will need to enter your administrator password. Click **Turn On FileVault**. The next screen will display the disk's recovery key. If you forget your password, this is the ONLY way to recover the data on the encrypted disk. Please write this 24 character string down and save it in a secure place. Click **Continue**. The next screen will ask if you wish to store your recovery key with Apple. For security's sake, we advise you to select the button labeled **Do not store the recovery key with Apple** and click **Continue**. You will then be prompted to restart your device to enable FileVault and begin encrypting the disk. Click **Restart**. Once you log back in, your device will encrypt the disk in the background.

Only install the software you need; and then, only from trusted sources

The fewer programs a device has on it, the fewer opportunities there are for something to go wrong. Your work computers should be kept lean, with only the applications necessary for work and your day-to-day tasks. Each of these programs should have been downloaded or purchased from trustworthy sources.

Uninstall software you don't use

A coda to the previous best practice. If there is a program on your device that you never use, uninstall it. That is one fewer program you need to keep updated.

Keep Bluetooth turned off unless you are using it

Bluetooth allows you to link your computer to nearby devices. This is extremely useful if you are trying to share files from your computer with someone. However, these networks also allow intruders easy access to your device. For this reason, they should always be turned off unless you are actively using them.

Do not share access to your device

This is security 101, but no one should be able to access your device. If you do need to share your device with someone, it must be a trusted individual and, ideally, it will be under your supervision. After you no longer need their assistance, you should change your login password.

Be aware of "shoulder surfing"

Penetrating a computer's defenses is not necessary if you are broadcasting sensitive information on your screen. If you are handling sensitive data, be aware of your surroundings and potential spies looking over your shoulder.

Lock your notebook whenever you step away

All these steps will be completely undone if you leave your device unlocked and unsupervised. An unlocked device is an invitation to any intruder to the data on your device as well as your network. Even if you're just grabbing a coffee, lock your computer.

Use a VPN on an unknown WiFi network

If you work from home or while you are traveling, you should use a trustworthy VPN service to encrypt your Internet connection. Unknown WiFi networks and public hotspots present all types of security vulnerabilities that can be avoided with a VPN.

Use antivirus software and set up periodic scans

Antivirus software will help you identify and remove any malware that gets on your system. It is an essential part of keeping your device clean and free of malicious programs. Windows 10 comes with antivirus software already installed, called Windows Defender Antivirus. To access it, press **Windows Key + C** and select **Settings**. Once the Settings window opens, select **Update & Security**. This will automatically take you to the Windows Update page. Click Windows Security. Once the **Windows Security** window opens, click **Open Windows Defender Security Center**. A new window will open. Click **Virus & Threat Protection**. Here you can run a system scan or adjust the settings of Windows Defender.

Use Acrobat Reader with Protected View mode to access PDFs

Hiding malware in PDF attachments is becoming one of the more common ways hackers deliver malware onto a system. Therefore you must be careful anytime you are opening a PDF file. Acrobat Reader has enabled its Protected View mode by default. When a PDF file is opened in Protected View, all the operations Acrobat Reader needs to run to display the PDF are run in a restricted manner inside a confined environment. That way, if there is a malicious program hidden in the file, it is contained and cannot infect your device.

Smartphones

As more and more business is handled remotely, our smartphones are becoming more and more integral to our work — and therefore, to cybersecurity. While it is easy to overlook smartphones, they often have the same access to sensitive data and corporate networks as work computers.

Keep your mobile phone operating system and apps up-to-date

Same as your computer, the software makers for smartphones are continuously finding flaws and putting out fixes in the form of updates. If an app or your operating system has not been updated recently, your device could be vulnerable to exploitation.

Enable full device encryption

Since we take our smartphones with us everywhere, they are much more likely to be lost or stolen than a computer. Now that smartphones have more storage than some early computers, they could potentially expose a significant amount of data. Encrypting your device will protect the information on your device unless it is unlocked.

Android

To encrypt your Android device, tap Settings and then Security (remember, the phrasing on each Android device might be slightly different). Here you will see the option to encrypt your phone. (NOTE: the encryption process can take over an hour, and your phone has to be plugged in.) Once your phone has been encrypted, you will have to enter your PIN or passphrase to decrypt the data each time you restart the phone.

Apple

The latest iPhones (any after the 3GS) and all iPads automatically encrypt the device's data, but you must set a passcode. For devices running iOS 9 or later (remember to **keep your operating system up-to-date!**) tap **Settings** and then tap **Touch ID & Passcode**. You will then be prompted to create a six-digit passcode. Once your passcode is created, scroll to the bottom of the Touch ID & Passcode screen. You should see a message saying "Data protection is enabled." This means that your device's encryption is tied to your passcode and only your passcode can unlock the data on your phone.

Set a strong PIN code or passphrase

Despite the many advances in ID verification technology, PINs and passphrases are still your most secure option. Biometric methods, like fingerprint or face scanners, are not always protected by law, which means a law enforcement officer could force you to unlock your phone. People rarely make their pattern lock complex enough for it to be secure, and it is easier for someone to figure out your pattern from looking over your shoulder. Androids allow you to make passwords (or passphrases — more on that below) of up to 16 characters, and iPhones and iPads enable you to make alphanumeric passcodes, combining letters, numbers, and symbols. Experts suggest using a passcode of at least eight characters, and those characters should be a mix of numbers, capital letters, and lowercase letters.

Limit the information accessible from the lock screen

Certain apps send updates that you can read without having to unlock your phone. Same for text messages. This means that your passcode does not protect this information. If your device is stolen or lost, an intruder will be able to read the texts you receive even if they cannot access the rest of the data on your phone.

Android

To adjust the notification settings on your Android device, tap **Settings** and then **Notifications**. Then by tapping on each app, you can decide what information they show while the device is locked.

Apple

Adjusting the notification settings on your iPhone or iPad is slightly trickier. For apps that come with the phone (like the Calendar) tap **Settings** and then **Control Center**. Then tap **Access on Lock Screen** to turn the option off. To stop your text messages from being displayed on the lock screen, tap **Settings**, then **Notifications**, then **Messages**. On this screen, tap on **Show on Lock Screen** to turn the option off. To prevent apps from sharing data on the lock screen, you must turn each one off individually by tapping that app's entry in the Notifications screen.

Disable your Voicemail unless you absolutely need it

Voicemails are typically only protected by a four-digit PIN, leaving them vulnerable to being bruteforced. Once an attacker has access to your voicemail, they can request a password reset over the phone number at times when they think you are unlikely to answer. If you miss the call, the reset code will be recorded in your compromised voicemail and the attacker can use it to access your account and lock you out. This also bypasses two-factor authentication. The best defense against this is to shut down your voicemail. If this is not an option, then use the maximum amount of allowable characters for your voicemail PIN, make sure the code is random, and do not use your phone number or phone calls for password resets.

Do not share access to your device with anyone

Any time you share your device with someone else, you are increasing the odds of the device being compromised or your login credentials being shared. If you need to share your device, share it only with someone you trust and, ideally, supervise them. Once they are finished with your device, you should change your passcode

.

Keep Bluetooth and NFC turned off unless needed

Bluetooth and near field communications (NFC) allow your devices to link and share information with other nearby devices. This is extremely useful if you are trying to share files from your phone with someone. However, these networks also allow intruders easy access to your device. For this reason, they should always be turned off unless you are actively using them.

Passwords

Passwords are the keys to an account. They are a free, simple, and effective way for your employees to prevent unauthorized access to their devices or accounts — provided they use strong, unique passwords.

Use unique, strong (at least 16 characters) passwords for every account

A strong password is one that is unlikely to be cracked or guessed, which means that items like your birthday, your address, or the word "password" should be immediately dismissed. To be strong enough to avoid being cracked by a computer, a password should be at least 16 characters. An alternative to using a password is to use a passphrase. These are more memorable. We advise using a passphrase of at least four obscure words with numbers and characters mixed in. A passphrase like "llama9cakeenn!uilima" is extremely difficult for a computer to crack because it contains a large amount of entropy. But it is easier for a human to remember because it is only four words ("llama", "cake", "ennui", and "lima") with two extra characters, the placement of which can be memorized.

Just like you do not use the same key for every lock, you should not use the same password for every account. If you use unique passwords for every account, then even if one password is cracked, the rest will remain secure.

Finally, your passwords should never be written down or out in the open where anyone could access them.

Use a password manager

While passphrases will help make your passwords more memorable, eventually you will have too many accounts to possibly remember a strong, unique password for each. At this point, you should start using a password manager. A password manager securely stores and auto-fills all the passwords for your accounts and thus could also protect you from phishing attack. They can even assist you in creating strong passwords for new accounts. To access these passwords, you type in a single, master password. This way, instead of remembering dozens of passwords, you remember one and your password manager remembers the rest.

Use 2FA wherever possible

Two-factor authentication adds an extra identity verification to the standard login procedure. Instead of just typing in your username and

password to sign in, 2FA requires you to provide another type of credential (a second factor) before you can access your account.

The secure types of 2FA use a time-based, one-time password that is generated by a zero-trust app, such as Authy, DuoMobile, or Google Authenticator, or a physical fob, such as Yubikey.

Store your 2FA codes in a secure place

Each time you set up 2FA on an account, that account will provide you with a set of one-use codes that you can use to log in to their service in case you cannot, for whatever reason, enter the correct form of second verification. These codes need to be stored in a safe, easily accessible place so that you have a backup and can open your accounts even if you have lost your phone or Yubikey fob.

USB peripherals

USB flash drives are a convenient way to store and share data, but they must be treated with caution. Because it is impossible to know what is on them without plugging them in, that makes them ideal vehicles to deliver malware onto devices.

Do NOT use unknown USB devices or sockets

Just like you would not stick an unknown substance into your mouth, you should never plug an unknown USB drive into your computer. If you do, you let an intruder bypass your firewall and get direct access to your device. If you find a USB drive, give it to a member of your IT team or a tech expert so that they can scan it.

This same caution should be used for USB sockets as well. If you do not know who is in charge of running a public USB socket, like the ones you see at charging stations, you should not plug your device into it. These sockets can also directly access your device.

These best practices will protect you only if they are implemented 100% of the time. This requires creating a culture of IT security awareness.

The most important thing to remember is that creating a workplace culture of IT security awareness requires buy-in from employees at every level. If management doesn't view IT security as a priority, then lower-level employees won't either.

Employee IT security best practices

This list should be shared with your employees so they always have an easy, ready-made guide listing the steps they can take to improve their IT security.

Area	Security best practice
Notebook	Keep your operating system and software up-to-date
	Enable a local firewall to block incoming network connections
	Enable full disk encryption
	Only install software you need and only from trusted sources
	Uninstall software you don't use
	Keep Bluetooth turned off unless you are using it
	Do not share access to your device
	Be aware of "shoulder surfing"
	Lock your notebook whenever you step away
	Use a VPN on an unknown WiFi network
Windows only	Use antivirus software and set up periodic scans
	Use Acrobat Reader with Protected View mode to access PDFs
Smartphones	Keep your mobile phone operating system and apps up-to-date
	Enable full device encryption
	Set a strong PIN code or passphrase
	Limit the information accessible from the lock screen
	Disable your voicemail unless you absolutely need it
	Do not share access to your device with anyone
	Keep Bluetooth and NFC turned off unless needed
Passwords	Use unique, strong (at least 16 characters) passwords for every account
	Use a password manager
	Use 2FA wherever possible
	Store your 2FA codes in a secure place
USB	Do NOT use unknown USB devices or sockets

Chapter 3

Enforce email security

READ THIS CHAPTER to understand the email security best practices regarding:

- Phishing attacks
- Imposters spoofing your email
- Email security best practices list

Email security is vital to your business's overall IT security because it is the most common attack vector. Phishing emails and fraud are two attacks that do not require any technical skill, merely an understanding of human nature, a flair for deception, and an email address. Fooling a human into clicking on a malicious link is a much easier way to penetrate a network than trying to hack its firewall.

Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.

Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.

Receive an email?
DON'T GET PHISHED

Phishing is a type of cyberattack in which a hacker, pretending to be a trusted individual or organization, tricks the victim into opening a malware-containing email.

This can have terrible consequences for your business, including loss of confidential data, leak of financial information and identity theft of your employees' data.

The greatest security threats faced by organization:

Phishing attacks are the most pressing cyber security challenge

Source:
Cyberark, IT security professional respondents, multiple responses allowed

83% of global infosecurity respondents experienced phishing attacks in 2018

Source: "State of the Phish Report"

Top phishing targets by industry:

Email remains the most popular method of phishing attack

Phishing

Phishing is by far the most common type of IT security threat your business will face. It involves someone posing as a legitimate customer, institution, or colleague to fool your employees into sharing sensitive data, such as business financial details and passwords, or clicking on a malicious link that will compromise their device.

Phishing takes many different forms. Recently, it was reported that Google and Facebook were scammed out of over $120 million by someone who sent forged contracts and invoices asking for payment. Or, in what is probably the most infamous example of phishing, the campaign manager of Hillary Clinton's presidential bid was fooled into clicking on a malicious link and entering his Google password. This exposed his entire Gmail inbox.

Phishing can also involve texts and instant messages, but given email's ubiquity, it is by far the most common medium.

How to prevent phishing

Training

Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. This training should be continuous as well. Phishing attacks are always evolving.

Create a process

Your business will receive phishing emails. So eventually, someone will fall for one. If this happens, your company needs to have a process in place that everyone knows and understands. An employee must know whom to speak with if they think they were just phished. By acting swiftly, you can mitigate the damage of a phishing attack.

Limit public information

Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories, including phone numbers or physical addresses. All these pieces of information can help attackers engineer an attack.

Carefully check emails

First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the "From" address to see if it is odd (e.g., service145@mail.145.com). If an email looks suspicious, employees should report it.

Beware of links and attachments

Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. Attachments are especially dangerous because they may contain malware, such as ransomware or spyware, that can compromise the device or network.

Do not automatically download remote content

Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it.

Never share sensitive information without being sure who is on the other end

No organization should EVER ask for your password via email. If an email is asking you to send your password, credit card number, or other highly sensitive information in an email, this should be a red flag.

Hover over hyperlinks

Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL. You can retrieve the original URL using this tool.

If in doubt, investigate

Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email.

Take preventative measures

Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims

to come from, making it easier to identify potential phishing attacks.

What to do if your company is phished

Follow your company's procedures

Your company must have a process in place for employees who think they may have been fooled by a phishing email. The first step should be reporting the phishing email and any data that was shared to your organization's IT security leader.

Limit the damage

Once your organization understands what the phishing attempt looked like and what information was exposed, your IT security leader should immediately change the compromised passwords. It may also be necessary to disconnect that employee's device from the network to prevent the spread of malware.

Alert others

Your IT security leader should also warn the rest of your employees that there has been a successful phishing attempt and tell them exactly what to look for. Once a phisher sees success with one employee in an organization, they'll often target others to increase their access. You should also inform the company or person that was impersonated that their identity is being used in a phishing scheme.

Notify customers if necessary

If the data exposed affects your clients, make sure you notify the affected parties — they could be at risk of identity theft.

Notify authorities

American businesses should report phishing attacks to the local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You can also forward phishing emails to:
spam@uce.gov (an address used by the FTC) and to **reportphishing@apwg.org** (an address used by the Anti-Phishing Working Group).

Imposters spoofing your email

This is when an attacker sets up an email that is identical to your business email address and sends out phishing attacks that appear to originate from your company. This degrades the trust your vendors and customers have in your company.

How to prevent your email from being spoofed

Use email authentication

This type of technology allows a receiving server to verify that an email you sent actually came from your company. This makes it much more difficult for scammers to impersonate organizations.

Domain-based Message Authentication, Reporting, and Conformance, or DMARC, is one of the primary ways to detect spoofed emails. DMARC can also be configured so that you are alerted anytime someone receives an email that appears to be a spoof of your domain.

ProtonMail also has advanced security features, like Authentication Logs, Encrypted Contacts, and Address Verification. Authentication Logs allows you to monitor if anyone else has logged in to your account. If you detect another user on your account, or an active session on a device you don't control, you can remotely log out. Messages sent between ProtonMail accounts are only vulnerable if a hacker compromises the end-user or stages an elaborate man-in-the-middle attack. Encrypted Contacts and Address Verification make it much more difficult for these types of attacks to succeed. These advanced features make it harder for anyone to access, tamper with, or impersonate your emails without your knowledge.

Keep your programs and apps up to date

A hacker could also access your emails through a compromised network. Always keep your security patches up to date and continually update your apps and programs so that you are using the latest version. Ideally, you should set them to update automatically.

What to do if your email is spoofed

Notify customers

If you discover that hackers are spoofing your business's email and using it for phishing attacks, you must tell your customers as soon as possible — by mail, email, or social media. You should inform your customers what your legitimate emails look like, what types of information your company will and will not request, and any other information they can use to spot phishing emails.

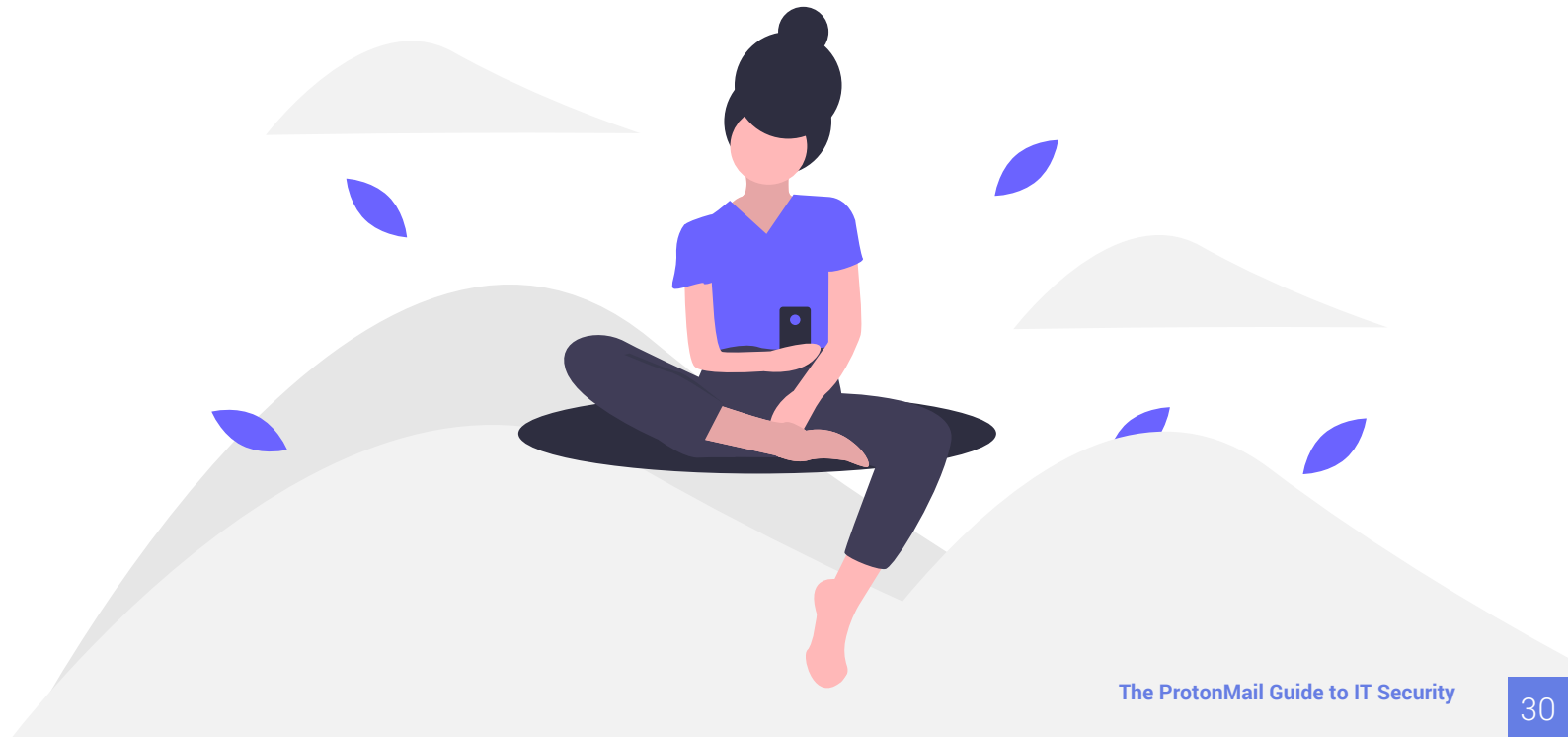
Notify authorities

American businesses should report spoofed emails to the local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint.

Employee email security best practices

This list should be shared with your employees so they always have an easy, ready-made guide listing the steps they can take to maintain email security.

Security best practice
Know how to identify phishing emails
Be aware of the dangers of email attachments
Inspect links before clicking on them
Disable the loading of remote content
Think carefully before using “Reply All”
If in doubt about an email, investigate further
If still in doubt, report suspicious emails to your IT security leader
If you fall for a phishing scam, **REPORT IT IMMEDIATELY**



Chapter 4

Protect your network

READ THIS CHAPTER to identify the IT security best practices your IT security leader should be in charge of, including:

- Network security basics
- Creating a secure internal network
- Maintaining user security
- Log auditing
- Advanced network security
- Data backups
- IT security admin best practices list

Network security sounds complicated, but at its heart, it is straightforward. Similar to how you lock up your office, you must lock up your network to keep your data safe. You must be able to prevent and react to the unauthorized access to and abuse of your network. This requires having technological solutions, documentation, processes, and an IT security leader or admin to control the flow of information over your company's system. While this IT security leader should be able to handle the more technical aspects of network management, their job is impossible unless your staff regularly implements IT security best practices (See Chapter 3).

Your network encompasses all your devices, including computers, laptops, workstations, servers, tablets, or smartphones and all of their connections, either to each other over a local area network or to the Internet. This could be as simple as two laptops sharing documents over the cloud or as complex as companies that have their own internal networks running off private servers.

This chapter gives a basic outline of the responsibilities of your IT security leader (See Chapter 1) and what they should do to maintain your network security.

IT security leader basics

Just as every company handles different data, each company faces unique threats. Precautions that would make sense for one company may not be necessary for another. For example, most small businesses that are not focused on information technology do not need to concern themselves with an internal network or a firewall or a SIEM. Instead, they should focus on taking simple steps that can significantly reduce their business's vulnerability.

Train employees on IT security

The most critical step is training your staff and cultivating a culture of IT security awareness. (See Chapter 3)

Remind employees about phishing attacks and describe new threats

IT security threats are constantly evolving. Hackers are continually exploiting new bugs and creating new types of social engineering attacks. Keep your employees and colleagues up to date by sending out a brief email update on the latest and most popular threats. These updates will help them recognize any hacking or phishing attempts they might encounter.

Conduct a brief assessment of employee adherence to the Employee IT security best practices list

Without regular tests and reminders, even the most conscientious employees can forget about IT security best practices. Conduct a simple test or hold a brief meeting to make sure your employees and colleagues are adhering to IT security best practices. These evaluations or meetings are also an excellent time to address any questions about IT security your employees or colleagues might have.

Create a database of approved devices

But before the training even begins, your IT security leader should create a comprehensive database of all the devices that connect to your company's network or have access to its data. Each one of these devices is a potential weak point. Your IT security leader should ensure that all network-connected devices, including smartphones, are using a firewall and full disk encryption.

Establish permission levels for employees and devices

Once you know which devices will be connecting to your network, your IT security leader should create different levels of access to your company's data, depending on what that employee does. This includes physical access to sensitive network devices and hard-copy files. No employee should have access to portions of data that are not essential to their day-to-day tasks. Only pre-approved employees should be able to download or install new programs on their device.

Use privacy-focused services

Look into replacing software or applications that your business uses to handle sensitive data with privacy-focused services. These types of programs or apps generally use end-to-end encryption (E2EE) to keep information inaccessible except to its owner (and, depending on the service, its intended recipient). Chapter 5 has a comprehensive list of a range of privacy-focused services your business can use.

Creating a secure internal network

As your business grows, you will need to adjust your IT security precautions. Eventually, you will need to start putting in place technological tools, like your own business WiFi network, internal servers, and a firewall. This will also require an IT security leader with more technical expertise as well.

You should follow the steps below as your business grows. Using a secure WLAN can be done by companies of any size, but implementing a firewall, segmenting your network, or using a corporate VPN only apply to businesses that run their own internal network.

WLAN Security

Nearly every business needs Internet access to handle day-to-day tasks. To be secure, you need to have your own, dedicated WiFi router. All WiFi routers sold since 2006 use the WiFi Protected Access 2 protocol, which is currently the most secure. If you are concerned, check your wireless card or device for a "Wi-Fi CERTIFIED" label to see if it uses WPA2.

The next step is to make sure you use the Enterprise mode of WPA2—also known as 802.11i. This is more complex to set up than a standard WiFi network, but it offers several essential security advantages, the most important of which are the elimination of shared passwords and WiFi snooping.

Set up a network firewall

A properly configured firewall is your internal network's first line of defense. It filters the data of your network or device and only allows permitted traffic through. If your corporate network is connected to the Internet, a perimeter firewall will prevent bad actors from accessing your network by blocking traffic that doesn't meet a predetermined set of criteria.

Segment your network

Segmenting your network is the best way to prevent a full system failure from occurring if a malicious actor or malware make it past your firewall. If your network is segmented, even if one server is compromised, the malware can be contained, and the rest of your IT infrastructure can continue functioning. You should base the decision of how to segment your network on the sensitivity of the data being handled and where the traffic is initiated. A server that is accessible from the Internet should not be located on the same network as a server containing sensitive data.

There are three ways you should think about segmenting your network: using Network address translation (NAT), maintaining separate WiFi networks for employees and guests, and creating virtual local area networks (VLAN).

Your employees' devices should not have their own, public IP addresses. NAT allows several computers on the same network to share one public IP address at the same time. If your company employs a dynamic NAT, you add another layer of protection between your internal network and the Internet, as the NAT will only allow connections that devices from your system initiate.

Your business WiFi network should not be shared with guests. Even with WPA2 Enterprise, allowing untrusted devices onto your WiFi poses the risk of introducing malware into your network. Restricting visitors to a separate WiFi network segment will also prevent them from accessing internal services, such as network files and printers. Finally, it gives you a greater measure of control over your guests' WiFi without affecting your employees' WiFi.

Finally, make sure your employees' devices and your corporate servers are connected to different VLAN. A VLAN is an example of software-defined network segmentation. It partitions and isolates parts of a single physical network so that network applications can be kept apart.

Use a corporate VPN

A firewall will protect and segment your network, but today, more and more employees are working remotely. You need to find a way for them to securely access your corporate data so that they can do their jobs. This is different from a VPN service that will encrypt your Internet connection. While it will use the same type of protocols (OpenVPN or IKEv2), a corporate VPN creates an encrypted connection over the Internet to your company's corporate server, letting your employees safely download and transmit files without any fear of malicious actors intercepting or manipulating your data.

Advanced IT security leader best practices

Once your company has established its own internal network, your IT security leader's responsibilities will dramatically change, as will the expertise necessary for the job. In addition to keeping your staff trained and up to date, they will have to work much more extensively with the technological tools you have put in place to secure your system.

Maintaining user security

Reassess role-based access management and separation of duties

Companies are not static. New employees come, old employees are promoted, projects end and new ones are reassigned. The turnover of the business cycle means that the type and amount of data that an employee should have access to is continuously shifting. By keeping employees' access limited to only the data they need to perform their day-to-day tasks, you reduce the chance of a catastrophic breach if one account is compromised. Your IT security leader should regularly assess which employees have access to which data and confirm with their supervisor that that level of permission is appropriate. Role-based access control will need to be implemented to define which user is allowed to access which data.

Disable old or obsolete accounts

Old, unused, and inactive accounts are a security threat. Your admin must disable them in a regular and timely manner.

Always check to make sure there is not a reason these accounts have been inactive (like that employee is gone on vacation or parental leave). Also, check to see if any employees have recently been fired or quit, and have them added to the list. Once the list is prepared, and your IT security leader has double-checked it, they should go through and disable user accounts one at a time.

Log auditing

Review security information and system logs (with a SIEM, if applicable)

Every device on your company's network should produce comprehensive event logs that you can search, filter, and review. These logs will help your IT security leader catch any emerging issues or security threats early on.

These reports should all go into a centralized location. By having the reports and records all in place, you can search for abnormal behavior and make sure they are not modified by accident or deleted or altered maliciously.

A SIEM (security information and event management) system aggregates data from

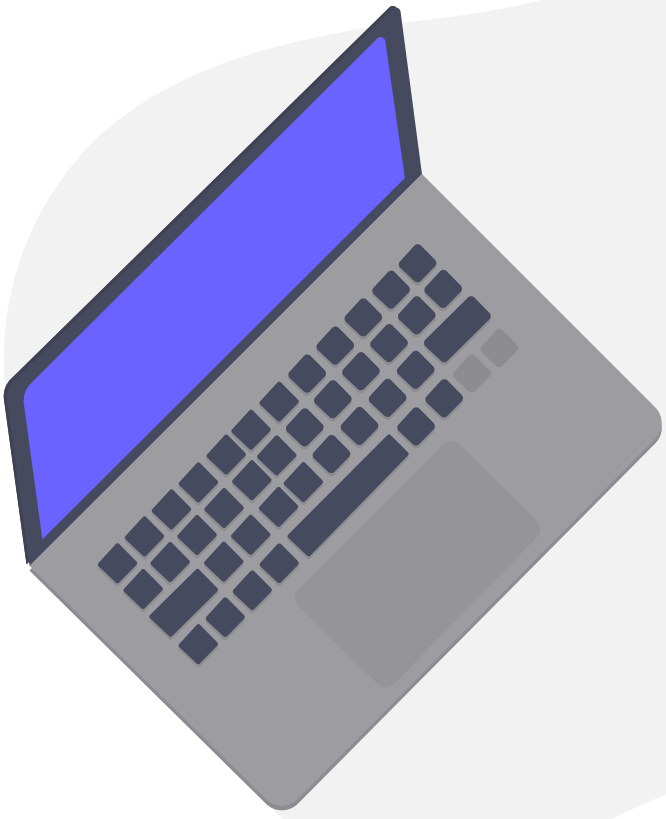
your network and uses rules-based or statistical correlation engines to determine what normal activity on your network looks like, identify any deviations, and take appropriate action. A SIEM system also allows you to view in one place all the logs and records your network generates, making it much easier to spot suspicious patterns. While this is a more advanced tool that should be employed on larger networks, if your company's network does have a SIEM system, check it regularly.

Whether your IT security leader uses a SIEM or manually checks your system's logs, they should do it on a regular basis to make sure nothing unusual has been detected and to make sure the logs are being recorded as expected. If an attack or a failure happens and they do not have any records to go over, it will be difficult to find and solve the problem.

Review user activity and remote access logs

The easiest way to start spotting suspicious activity is by looking at who is logging in and from where. If someone is logging in remotely after you just saw them in the office, or if someone who has been fired has just logged in, there may be foul play involved. Your IT security leader should regularly review these logs, flag all suspicious logins, and follow up by contacting the account owner to find out what they were doing. If the employee is unaware of the login or has reason to think their account may have been compromised, your IT security leader should check to see if any sensitive data was accessed and take measures to ensure the account's security (like changing its password or temporarily suspending the account).

- Flag any suspicious logins.
- Record who was involved, what happened, and when it happened.
- Check to see if any sensitive data was accessed.
- Take action to secure data/account.



Advanced network security

Check computer lifecycle and update as necessary

Your list of all network-connected devices must expand to include all your business's servers and workstations. This inventory should be updated anytime new systems or hardware are integrated into your network.

Check software lifecycle and update as necessary

In addition to a list of all your devices and hardware, you should maintain and append a comprehensive list of all the software you are using on them, along with their most recent update. Software updates are often released to fix known bugs. By using an old version of a program, you are introducing a vulnerability into your system. This inventory should be updated anytime software or applications are integrated into your network.

Your IT security leader should also regularly check online to see if there are new versions of any of the programs you are using. If one has been updated, then download the update (or email fellow employees to download the update). Then open up your software inventory and add the details of this update, new program, or application.

Check and install latest security patches (with SCAP, if applicable)

Failing to carry out regular security patches is one of the most common points of failure in any computer network, and often holes appear as a result of bad processes in systems' maintenance.

SCAP, or the Security Content Automation Protocol, is an automated system that will scan your system searching for vulnerable versions of software. Using SCAP lets your company benefit from the entire SCAP community of IT security experts. They define the different configurations and use cases that SCAP should look out for, making SCAP a comprehensive vulnerability scanning tool.

Test your firewall security

Your IT security leader should regularly check your firewall security to make sure that your company's servers cannot be accessed from the outside through an unknown port.

They should run a scan to make sure the only ports on your network that are open are the ones they have whitelisted. Perform an external to internal port scan with Nmap.

- Check which ports are supposed to be opened.
- Perform a remote scan with Nmap and compare the result.

Evaluate firewall configuration

If the firewall security test did not perform as expected, then your IT security leader should evaluate the firewall configuration.

To make sure the firewall is configured properly, your admin should look at the different settings your firewall offers and adjust them to resolve the issue you found. To do this, they will need to also validate the authorized flow of traffic into your system as well as between internal zones (if applicable).

They should go through the sub-checklist below to troubleshoot the basic settings that might have caused the firewall security test to fail.

- Check anti-spoofing filters.
- Check user permit rules.
- Check system administrator alert settings.
- Check system traffic log analysis.

Test and run antivirus software

Antivirus is a preventative measure. It works to detect, quarantine, and remove any known malware that makes it on to your system. Ideally, your network will not be flooded with malware, and so it may be hard to know if your antivirus is doing its job sometimes. But given the essential role antivirus software plays in your overall network security, and especially for workstations or servers dealing with files, it is crucial your IT security leader tests your antivirus software regularly.

They can test the resilience of your antivirus software by downloading an EICAR file designed to simulate a virus or malware infection. EICAR files are completely safe and used by IT security experts to see if antivirus programs are working as they should.

Follow the process in the sub-checklist below.

- Download the EICAR file.
- Run an isolated scan for the EICAR file.

Your system's antivirus software should detect the EICAR file, alert you, and quarantine it. If it does not, you should strongly consider getting new antivirus software.

Following the EICAR test, perform a full system scan:

- Launch your antivirus software control panel.
- Perform a full system scan.
- Isolate and quarantine any threats detected.

Data backups

Making backups of your business's data is not necessarily part of network security. It is more like your insurance policy in case your network security fails. If ransomware compromises your company's devices or if there is a system failure, these backups will help your company get back on its feet.

Check and back up system data

Your IT security leader needs to make regular backups of all your most vital data. Remember, it is better to be over-inclusive than for a system crash to halt your business because you did not save the correct folder. Ideally, the backup process will be automated.

Even if the backup process is automated, your admin needs to regularly verify that all the processes are running smoothly and that the data are actually being saved.

- Ensure servers are fully backed up.
- Ensure workstations are fully backed up.

Making sure the backups are working and accessible is just as important as checking to make sure the data are being backed up in the first place. Using a random sample of files from the most recent backup, your IT security leader should try opening them on a workstation machine to see if the data are accessible. You should test at least three backup files to get a more reliable result.

- Take three backup images made in the last week.
- Load them all onto the same configuration as their parent system.
- Check they are all working as expected.

Evaluate backup process

If the backup files your IT security leader tested were inaccessible or corrupted, they must now locate the problem in your automated backup system. Finding the problem can require extensive testing at each stage of the automatic backup process, including re-saving and re-testing system-wide backup files or changing to a new automated backup process.

- Perform backup process troubleshooting.
- Test three more random backup samples.
- Evaluate your current backup process.
- Consider changing to a new backup process.

IT security leader best practices

Area	Security best practice
Basics	Train new employees on IT security (Chapter 3)
	Regularly review & introduce new IT security best practices with employees
	Create a database of approved devices
	Establish permission levels for employees and devices
	Use privacy-focused services (Chapter 5)
	Regularly remind employees about phishing attacks and describe new threats
	Regularly test employee adherence to the employee IT Security best practices (Chapter 3)
Creating a secure internal network	WLAN Security
	Set up a network firewall
	Segment your network
	Use a corporate VPN

Advanced IT security leader list of best practices

This list should be gone through every two weeks to cover the basics of IT security

Maintain user security	Reassess role-based access management and separation of duties
	Disable old or obsolete accounts
Log auditing	Review security information and system logs (with a SIEM, if applicable)
	Review user activity and remote access logs
Network security	Check computer lifecycle and update as necessary
	Check software lifecycle and update as necessary
	Check and install latest security patches (with SCAP, if applicable)
	Test your firewall security
	Evaluate firewall configuration
	Test and run antivirus software
Data backups	Check and back up system data
	Evaluate backup process
Hardware checks	Perform routine network maintenance

Chapter 5

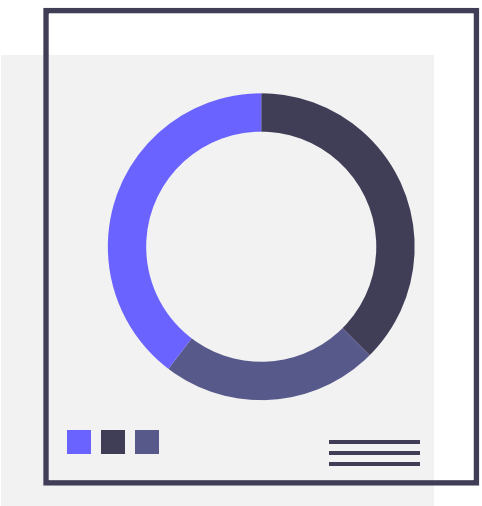
Adopt top IT security solutions for small businesses

READ THIS CHAPTER to see all the different apps, programs, and services that offer your company increased IT security and data protection. This list includes both free and paid services for

- Communications
- Storage
- Productivity
- Security
- Advanced network security

We made this the last chapter of our ebook because IT security is primarily about creating a culture of IT security awareness. Merely switching to encrypted services will not solve all of your IT security issues. The previous four chapters that describe how to implement IT security best practices form the foundation of a sound IT security policy. However, the following encrypted services will reduce your company's exposure, and, when paired with a security-conscious workforce, can go a long way to preventing a data breach or hack.

Note that while some of these tools will be good solutions for companies of any size, others will work best for smaller businesses that have not created their own internal network. We describe some tools that larger companies can use to secure their network (See Chapter 4), but other tools will require expert help to implement correctly.



Communication

Email provider

Most small businesses rely on emails to handle both their internal and external communications. Email security best practices are essential to keeping your business's data safe, but some email providers can offer your company more security than others.

ProtonMail

ProtonMail offers its users automatic end-to-end encryption. Your emails are encrypted before they leave your device so that only you and your intended recipient can access them. You can even secure your messages to non-ProtonMail users by sending password-protected emails.

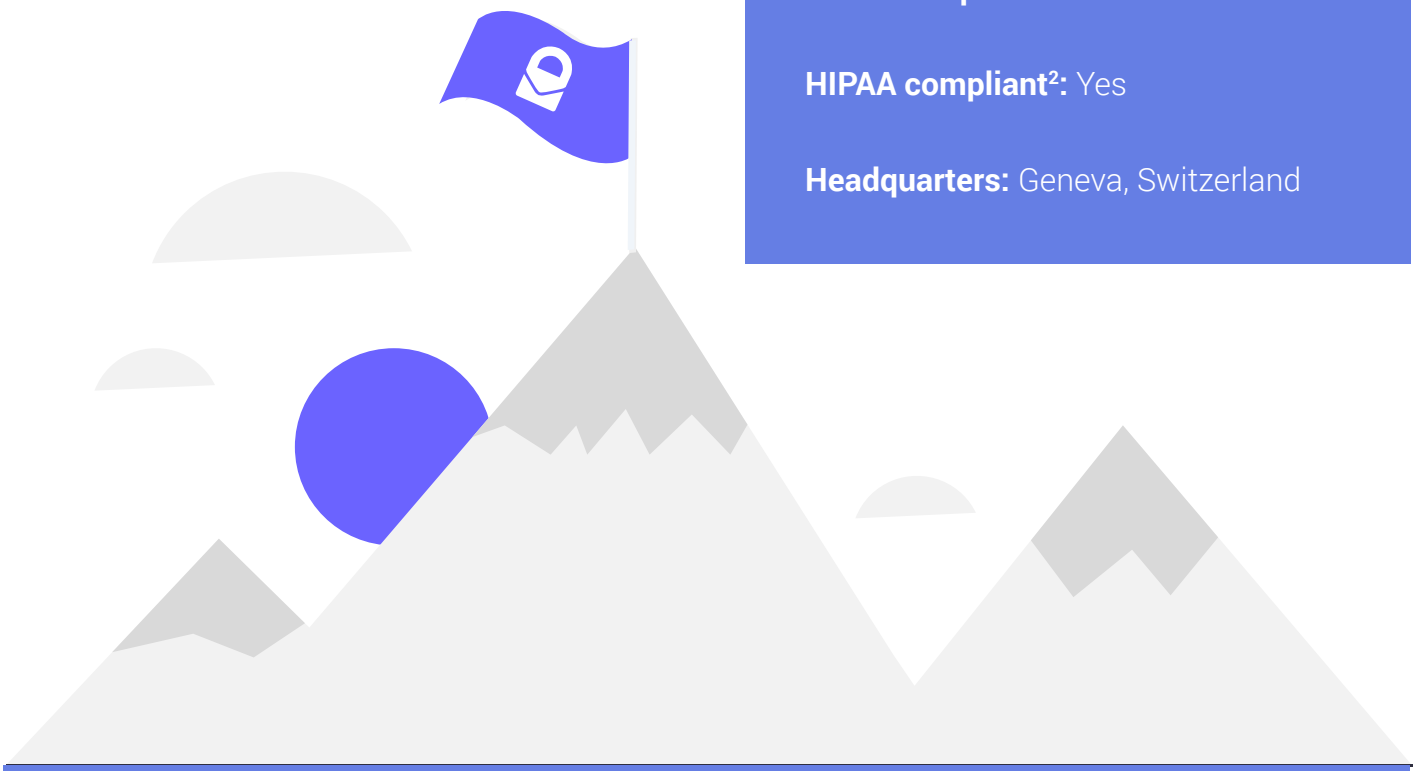
Platforms:
Android, iOS, and web app. Also has Bridge integration with Microsoft Outlook, Mozilla Thunderbird, and Apple Mail

Price: Has a free option. Premium plans begin at $5 per user per month.

GDPR compliant[1]: Yes

HIPAA compliant[2]: Yes

Headquarters: Geneva, Switzerland



1 This signifies that this tool adheres to the technical safeguards defined in the GDPR guidelines, which means that it can contribute to an organization complying with GDPR. It does not mean that just by using this tool your organization will be GDPR compliant.

2 This signifies that this tool adheres to the technical safeguards defined in the HIPAA guidelines, which means that it can contribute to an organization complying with HIPAA. It does not mean that just by using this tool your organization will be HIPAA compliant.

Team collaboration

Many businesses have employees and contractors working remotely. This can make coordinating a challenge unless you use a team collaboration app. Given the amount of information that can be exchanged and stored on these platforms, using one that is encrypted is a necessity.

Wire

Wire is one of the only end-to-end encrypted services that allows for group calls, which makes it more secure than Slack when trying to manage team communication. Wire has been independently audited and is entirely open source, giving you some assurance that Wire's code is doing exactly what they say it is.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at €6 per user per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Zug, Switzerland

Messaging

For companies that do not need all the functionality of a collaboration app but still want their communications to be secure, there are end-to-end encrypted messaging apps.

Signal

Signal is widely considered to be the most secure encrypted messaging app. It supports texts, group texts, as well as voice and video calls. Conference calls between more than two people, however, are not possible.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Free

GDPR compliant: Yes

HIPAA compliant: Yes (with caveats)

Headquarters: Mountain View, California, USA

Threema

Threema, unlike Signal, does not require a phone number to create an account, which means Threema is as close as you can get to truly anonymous messaging. The company headquarters is in Switzerland, giving its service strong legal privacy protections.

Platforms: Android, iOS, Windows phone, and web app

Price: Starts at 1.40 CHF per device per month

GDPR compliant: Yes

HIPAA compliant: No

Headquarters: Zurich, Switzerland

Storage

Cloud storage

Cloud storage has redefined how offices can work. By storing files on the cloud, your business can maintain a backup of all critical documents in case of a catastrophic system failure as well as easily share documents and sync progress between different employees. Protecting these files and the data they contain should be one of your business's top priorities.

Tresorit

Tresorit is an end-to-end encrypted cloud storage service. It has optimized its service for businesses, allowing you to create different levels of access for various documents and to revoke users' and devices' access to files.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Starts at $25 for two users per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Zurich, Switzerland

Sync

Sync is another end-to-end encrypted cloud storage service, similar to Tresorit. It gives businesses admin control, allowing supervisors to create different levels of access for different employees. Sync also allows you to preview your files before you open them.

Platforms: Android, iOS, macOS, and Windows

Price: Starts at $10 per user per month

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Toronto, Canada

Boxcryptor

Boxcryptor is slightly different. It allows you to encrypt your documents before you save them on a separate cloud service, like DropBox or Google Drive. Your team can still easily collaborate and share files over the cloud, but now your documents are secure.

Platforms:
Android, iOS, Linux, macOS, Windows, and a Chrome web browser add-on

Price: Starts at $600 for five users per year. (There is also an individual Business plan that is $96 per user per year, but it has less functionality.)

GDPR compliant: Yes

HIPAA compliant: Yes

Headquarters: Augsburg, Germany

Cryptomator

Cryptomator is the free, open source version of Boxcryptor. With Cryptomator, your employees can create a virtual hard drive that is connected to a folder (called a "vault") on their cloud storage service and protect it with a password. Any document they drag and drop into the virtual hard drive is automatically encrypted and backed up in the vault. There is also Cryptomator Server, for larger businesses

Platforms: Android, iOS, macOS, and Windows

Price: Free (There is a one-time fee of $9.49 to download the Android app and $9.99 to download the iOS app.)

GDPR compliant: Yes

HIPAA compliant: Yes

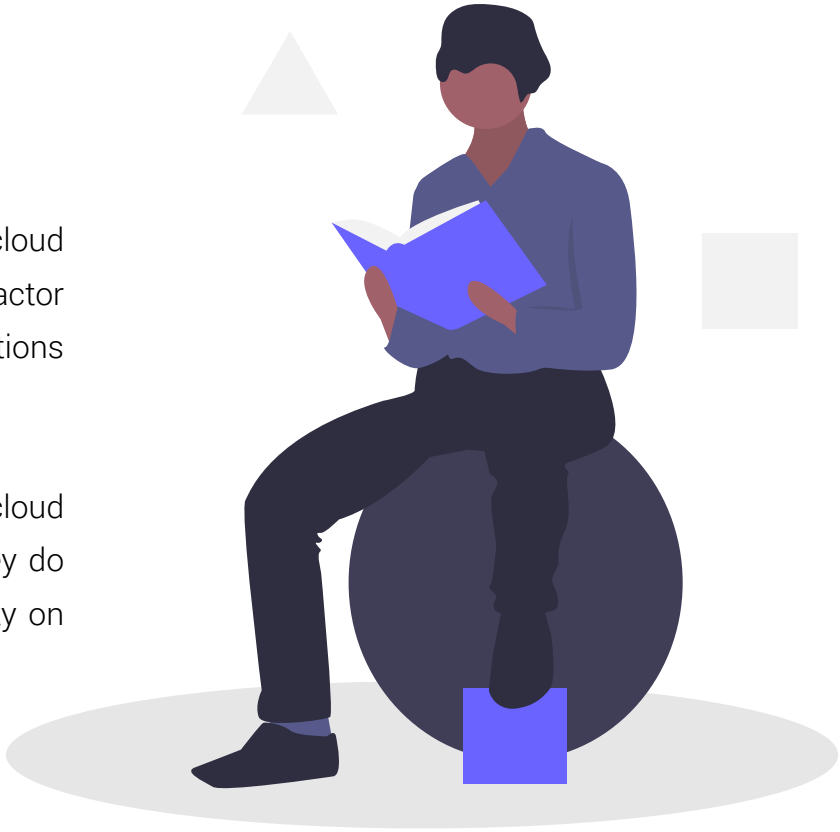
Headquarters: Sankt Augustin, Germany

looking to add encryption to the files on their company servers.

Other cloud services

pCloud is an end-to-end encrypted cloud service. It is GDPR compliant, allows two-factor authentication, and its business subscriptions start at $7.99 user/month/TB.

Spideroak is an end-to-end encrypted cloud storage service similar to Tresorit, but they do not offer two-factor authentication security on their accounts.



Productivity

Notepad

Also known as a "text editor," a notepad is a program that allows you to write and edit plain text. A notepad can be used to keep notes, write documents, and alter configuration files or programming language source code.

Standard Notes

Standard Notes is a simple, end-to-end encrypted note-taking app that can sync your notes across all your devices. Its clean interface and numerous extensions mean that you can use Standard Notes for everything from writing yourself reminders to coding.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Has a free option. Premium plans begin at $9.99 per user per month.

Headquarters: USA

Joplin

Joplin is another end-to-end encrypted note-taking app, but unlike Standard Notes, users must manually activate the end-to-end encryption feature. Joplin relies on external services, like NextCloud or Dropbox to synchronize across devices.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Free

GDPR compliant: Yes

Headquarters: N/A

Security

VPN

A virtual private network is an effective way to add a layer of encryption to your online activity. It also allows your employees to safely work on public WiFi while they are on the road.

ProtonVPN

ProtonVPN secures your Internet connection with AES 256-bit encryption, the industry gold standard, and its use of Perfect Forward Secrecy means that even if your traffic is intercepted and saved, it can never be decrypted at a later date.

Platforms: Android, iOS, Linux, macOS, and Windows

Price: Has a free option. Premium plans begin at $5 per user per month.

Headquarters: Geneva, Switzerland

Password manager

Creating strong, unique passwords or passphrases for your accounts is one of the basics of IT security, but no employee can remember all the passwords necessary to log in to all the platforms they need to use for work. (Look how long this list is already!) A password manager changes all that. By safely encrypting all your passwords, a password manager allows you to create passwords that are impossible to crack, without having to remember them all. Using a trustworthy password manager to secure your passwords is one of the easiest ways to improve your company's security.

Bitwarden

Bitwarden is an open source, end-to-end encrypted password manager. It helps your employees create randomly generated passwords for all of their accounts, and then syncs those passwords across all their devices.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at $5 for five users per month

Headquarters: Florida, USA

1Password

1Password is another end-to-end encrypted password manager, but it has a few more bells and whistles. While it is only a paid service, it is considered to be one of the most secure password managers. Its Watchtower feature will alert you if any of your passwords have been exposed in recent data breaches.

Platforms: Android, iOS, Linux, macOS, Windows, and web browser add-ons

Price: Starts at $3.99 per user per month

Headquarters: Toronto, Canada

Dashlane

Dashlane is also a premium end-to-end encrypted password manager. It will scan known security breaches and will send you an alert if it finds any of your passwords among those exposed. Its business plan also comes with an admin console that allows you to set permission levels for all your employees.

Platforms: Android, iOS, macOS, Windows, and web browser add-ons

Price: Starts at $4 per user per month

Headquarters: New York City, USA

Other password managers

LastPass: A premium password manager, but it does not alert its users if their password is exposed in a data breach.

KeePass / KeePassXC: These are both free, open source password managers, but neither of them offers official mobile apps.

Two-factor authentication

To ensure your critical accounts are secure, you should enable two-factor authentification (2FA) in addition to using a strong, unique password. The site Two Factor Auth will help you identify which services you can use 2FA on. By using 2FA on your accounts, you can prevent intruders from accessing your accounts even if they get a hold of your passwords.

YubiKey

The YubiKey is a hardware token (a specialized USB stick) that you can plug into your device to confirm your identity. While it is thought to be the most secure form of 2FA, relatively few services support hardware token 2FA.

Platforms: YubiKey 5 NFC works with macOS, Windows, and NFC-equipped Android and iOS devices

Price: A YubiKey 5 NFC costs $45.

Headquarters: Palo Alto, USA

Duo

Duo offers several 2FA solutions, including ones that incorporate Yubikey hardware tokens, confirmation requests delivered to the Duo app that foil man-in-the-middle attacks, and time-based one-time passcodes.

Platforms: Duo app is available on Android and iOS

Price: Has a free option. Premium plans begin at $3 per user per month.

Headquarters: Austin, USA

Other two-factor authentication services

Google Authenticator app: Google offers a free authenticator app that creates time-based one-time passcodes for 2FA purposes. It does not have the same functionality as Duo or a YubiKey. of them offers official mobile apps.

Disk encryption

All your devices should use some form of disk encryption to prevent unauthorized access to your devices' data storage in the event they are stolen or lost. By encrypting your smartphone or computer's hard drive, you turn your sensitive data into illegible code that can only be decrypted by your password. All the options discussed below are examples of disk encryption software.

VeraCrypt

VeraCrypt is an open source disk encryption service. Using VeraCrypt, your employees can encrypt the hard drive on their device, encrypt their USB flash drive, or even hide how much volume they have on their hard drive.

Platforms: Linux, macOS, Windows

Price: Free

Headquarters: N/A

Other disk encryption services

FileVault: FileVault is available on macOS X Lion and later. You can use it to fully encrypt your startup disk.

BitLocker: BitLocker is available on most Windows 7 and Windows 10 devices. It is a strong, full disk encryption service.

LUKS: LUKS is a free, open source hard disk encryption service for Linux.

Native encryption for Android and iOS: Any 3G iOS device or later and any Lollipop (5.x) Android devices or later are equipped with their own native disk encryption services. To learn how to encrypt your Android device, click here. To encrypt your iOS device, click here.

Personal antivirus software

Antivirus software (AVS) is a preventative measure meant to keep your devices clean. AVS scans your device for any malware, from ransomware to rootkits. If it detects any, it will attempt to remove them. More modern AVS also provides malware prevention measures.

Bitdefender

Bitdefender has strong antivirus protection, but it is light enough that it won't slow your device down. The AVS receives daily updates so that no malware can take it by surprise. They also have a more advanced option for larger offices. It will protect your servers and all your endpoint workstations without bogging down your network.

Platforms: Android, macOS, Windows are available free. iOS is available with a paid plan.

Price: Has a free option. Small office security starts at $99 for one year for five devices.

Headquarters: Romania

Advanced network security

5

This is just an introduction to some of the advanced tools for businesses that have their own internal network. These tools will help you secure your network, prevent vulnerabilities from arising, and help you deal with any threats or malware that make it past your defenses. Most, if not all, of these tools will require an IT expert to properly install and configure. If your company does not have its own internal network, these tools are not necessary.

Intrusion detection/intrusion prevention system

An intrusion detection/prevention system (IDS / IPS) monitors your network for malicious activity, policy violations, or malware. If it detects any of these, it will notify your IT admin or send a report to your security information and event management (SIEM) system (more on that down below). Depending on the threat it finds, your IDS / IPS could also attempt to stop the malicious activity.

Snort

Snort is an open source IDS/IPS that can perform real-time traffic analysis and packet logging on Internet protocol networks. It can also detect a number of probes and attacks and take action to stop them.

Platforms: Fedora, Centos, FreeBSD, Windows

Price: Free

Headquarters: N/A

Suricata

Suricata is also an open source IDS/IPS that can perform real-time traffic analysis. By using the extensive rules it has built-in, Suricata can scan for complex threats.

Platforms: FreeBSD, Linux, macOS, Ubuntu, UNIX, Windows

Price: Free

Headquarters: N/A

Network scanner

A network scanner searches your system for vulnerabilities in your security. If it detects a weakness in your network, it will send a report back to your IT admin. They will then use this report to address the found vulnerabilities and make the network more resilient.

Nmap

Nmap is an open source network scanner. In addition to finding network vulnerabilities, you can use Nmap to identify open ports to prepare for a network audit or to generate traffic to hosts on a network and measure their response time.

Platforms: FreeBSD, Linux (all distributions), macOS, Windows

Price: Free

Headquarters: N/A

Security Content Automation Protocol

SCAP is an automated system that will scan your system, searching for vulnerable versions of software. SCAP lets your company benefit from the entire SCAP community of IT security experts. They define the different configurations and use cases that SCAP should look out for, making SCAP a comprehensive patch scanning tool.

OpenSCAP

OpenSCAP is an open source SCAP system that will make sure your system is conforming to the policies and rules the SCAP community creates. With dozens of different policies, you can find the one that is right for your organization.

Platforms: CentOS, Debian, Fedora, Scientific Linux, Red Hat Enterprise Linux, Ubuntu

Price: Free

Headquarters: N/A

Security information and event management

A SIEM system aggregates all data from your network and then uses rules-based or statistical correlation engines to identify a baseline for what qualifies as normal activity on your network. It then searches for any deviations from this baseline. If it finds something it thinks is not normal, it will take action to stop it. It is also a repository for your IT admin to monitor and search your network records.

Prelude

There are two Prelude products: Prelude OSS and Prelude SIEM. Prelude OSS is a universal, free, open source SIEM system, but it is meant for smaller networks or for research. The more powerful Prelude SIEM is available for businesses and to secure larger and more complex networks. Both systems aggregate data from all your IT security tools, regardless of their brand or mark. They will work with either of the two IDS/IPSs on this list.

Platforms: Arch Linux, CentOS, Debian, Fedora, Gentoo, Mageia, Red Hat Enterprise Linux, Ubuntu

Price: The cost of a license for Prelude SIEM depends primarily on the number of devices that send their data to the system, whatever the volume.

Headquarters : N/A

OSSIM AlienVault

AlienVault is now part of AT&T Cybersecurity, but their open source SIEM system, OSSIM, is still available for free. In addition to letting its users collect and correlate event logs, OSSIM is connected to AlienVault's Open Threat Exchange, which allows users to report and receive updates about the latest malicious hosts. It also works with Snort and Suricata. Be careful because OSSIM is not a log management solution. If that is what you want, you would need to use either USM (paid version of OSSIM) or another log management system such as Elastic Stack.

Platforms: Must be installed on a virtual machine

Price: Free

Headquarters: San Mateo, USA

Elastic Stack

Elastic Stack, or its previous iteration, ELK (which stands for Elastisearch, Logstash, and Kibana, the three primary projects), is more of a data visualization system than specifically a SIEM, but it can be used as one. All the products in the stack are open source, and together they let you have a complete picture of your system and your employees' activity.

Platforms: Docker, Linux, macOS, Windows

Price: Free

Headquarters: Mountain View, USA

Network firewall

A network firewall is a network security system that monitors and controls incoming and outgoing network traffic between two or more networks based on a series of predetermined security rules. A firewall typically establishes a barrier between your internal network and other external networks, such as the Internet. A network firewall runs on your network's hardware.

OPNSense

OPNsense is the open source fork of the pfSense firewall software distribution. It can be installed on a computer or virtual machine to create a network firewall.

Platforms: HardenedBSD

Price: Free

Headquarters: Middelharnis, The Netherlands

iptables

iptables allows system administrators to configure tables, chains, and rules in the Linux kernel firewall. This gives the admin control over how data packets enter and travel around the system.

Platforms: Linux

Price: Free

Headquarters: N/A

firewalld

firewalld is an open source, dynamically managed firewall that allows you to establish different levels of trust around your network. It also works using the Linux system's iptables to filter data packets.

Platforms: Linux

Price: Free

Headquarters: N/A

Recommended IT security tools list

The ProtonMail IT security team recommends the following tools for small- and medium-sized businesses. A trained workforce that is vigilant for cyber threats is the most important IT security asset your company could have. That said, these tools will reduce your company's exposure by adding a layer of encryption to your communications, files, and operations.

Keep in mind that new tools — and threats — are being developed all the time. You should always keep an eye out for new products.

Area	Type	Recommended tools
Communication	Email provider	ProtonMail
	Team collaboration	Wire
	Messaging	Signal, Threema
Storage	Cloud storage	Tresorit, Sync, Boxcryptor, Cryptomator
Productivity	Notepad	Standart Notes, Joplin
Security	VPN	ProtonVPN
	Password manager	Bitwarden, 1Password, Dashlane
	Two-factor authentication	YubiKey, Duo
	Disk encryption	VeraCrypt
	Personal antivirus software	Bitdefender
Advanced network security	Intrusion detection/intrusion prevention system	Snort, Suricata
	Network scanner	Nmap
	Security Content Automation Protocol	OpenSCAP
	Security information and event management	Prelude, OSSIM AlienVault, Elastic Stack
	Network firewall	OPNsense, iptables, firewalld

Acknowledgements

This book, short and simple as it is, went through multiple rounds of checking by the Proton Technologies engineering, infrastructure, and security teams. It would not have been possible without the diligent double-checks and patient explanations of Alexis Coupe, Sebastien Ceuterickx, and Urs Schaufelberger. And a thank you to Marc Loebekken for making sure that everything passed legal muster.

The production of the book was truly a team effort. Richie Koch handled the researching and writing, Ben Wolford contributed to editing and corrections, Gabija Karpavičiūtė managed the development process, and Milda Šatė is responsible for the formatting and wonderful graphics employed throughout this book.

One final thank you goes out to the team at unDraw.co, which supplied many of the open source illustrations that we used in this book.

References

Page 6: 1. Verizon, 2018 Data Breach Investigations Report, 11th edition **2.** Netwrix, 2017 IT Risks Report **3.** Cisco 2018 Annual Cybersecurity Report **4.** Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton.A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate.Journal of Cybersecurity, 2018, DOI: 10.1093/cybsec/tyy006 **5.** 2017 State of Cybersecurity Among Small Businesses in North America, BBB, 2017

Page 13: 1. CyberArk, Global Advanced Threat Landscape Report 2018 **2.** Symantec, Internet Security Threat Report, 2019 **3.** Symantec, Internet Security Threat Report, 2017 **4.** Verizon, 2018 Data Breach Investigations Report, 11th edition

Page 24: 1. Knowbe4, 2018 **2.** FBI, 2017 **3.** PhishLabs, 2019, Phishing Trends & Intelligence Report: The Growing Social Engineering Threat **4.** Symantec, Symantec Internet Security Threat Report-2018, 2018