The ProtonMail Guide to IT Security

for Small Businesses

Create a culture of IT security

The ProtonMail IT security team

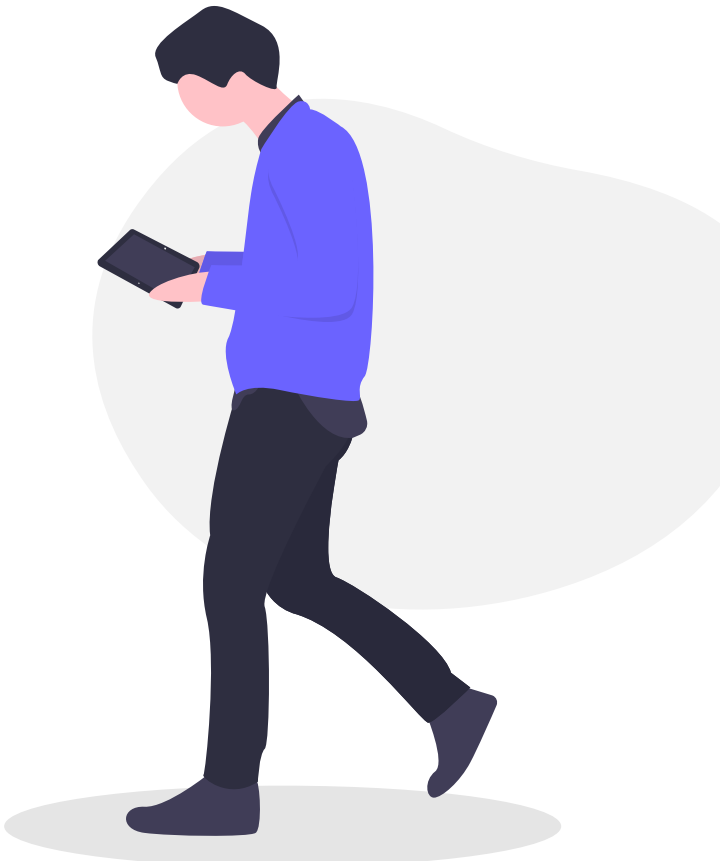
Create a culture of IT security

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** 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 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 3).

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 3) 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.

References

Page 2: 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.

ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click here.