**Email Privacy and Security Awareness**

**Table of Contents**

* Protect your data
* Protect your device
* Keep your email account secure
* Bad password habits
* Password best practices
* Social Engineering – Overview with examples
* Social Engineering Types
  + Tailgating
  + Quid Pro Quo attacks
  + Baiting
  + Pretexting
  + Phishing
  + Spear Phishing
  + Vishing
  + Smishing
  + Scareware
  + Shoulder Surfing
  + Whaling

**Protect your data:**

Protecting your data is the very first step in securing your digital life, therefore do not hesitate to take action.

Since the start of the Covid-19 pandemic, the number of cyber attacks on organizations and individuals has exploded.

**It is therefore more important than ever to keep your data and your privacy online safe.**

Here are some tips to protect your personal data online.

**1 – Remember physical security**

First of all, the quickest way to secure your data is to [protect your devices](https://blog.mailfence.com/protecting-your-devices/). Having physical access to a device makes it super-easier for an attacker to extract or corrupt your personal information. Do not leave your device unattended in public or easily accessible areas. Always keep your device password-locked (both while not being in use or after finish using it) and disable all lock-screen notifications (these are personal information, or email notifications that can pop-up throughout the day on your phone screen when it’s locked – You’ll find the way to turn them off in the Settings/notifications menu of your smartphone). Protect your device against physical theft. Also, keep your workspace safe : don’t leave your devices unattended on your desk. Be sure to lock your drawers if you keep your laptop or tablet in them.

**2 – Disable remote connectivity**

Some mobile devices are equipped with wireless technologies, such as Bluetooth. This means it can be used to connect to other devices or computers, and a hacker could easily reach your data this way. To ensure your privacy safety, you should get into the habit of disabling these features when they are not in use.

**3 – Encrypt your files to protect your information online**

If you are storing personal or corporate information, see if your device offers the option to encrypt the files (We’ve indicated several tools below). An [encrypted file](https://blog.mailfence.com/end-to-end-email-encryption/) means that the file is scrambled with a “key”, i.e. thanks to a secret code that only you (and the people to whom you give access to this file) know. This technique allows you to secure your data by hiding them in a cryptic text. Even if a hacker or unauthorized people can get access to your file, they won’t be able to read it. Be cautious, though when using encryption : you must remember your passwords and passphrases. Because if you forget or lose them, you may lose your data.

**4 – Be cautious with public Wi-Fi networks**

Before you connect to any public wireless hotspot – like on an airplane or in an [airport, hotel, train/bus station or café](https://blog.mailfence.com/protecting-your-devices/), keep in mind their network could not be as secure as it should be. In this case, your data will no longer be safe and it will be very easy for a malicious person to intercept it. When you want to surf on a site where you may have to give personal information, it is best to wait until you have access to a secure wi-fi network to ensure that your online privacy will not be threatened.

For all the cases where you need to connect to an unknown wi-fi network, follow these tips:

* Confirm the name of the network and exact login procedures with the staff to ensure that the network is legitimate.
* Only connect to sites which URL begins with “https://” when online shopping or banking.
* Use your own mobile network connection whenever possible : it is generally more secure than using a public wireless network.
* [Use a Virtual Private Network (VPN)](https://blog.mailfence.com/vpn-secure-email/) which will hide your personal data from others people using the same public network. Chose a legitimate VPN service known to respect privacy.

And for your data safety, once again, don’t forget : refrain from doing online shopping, banking, or sensitive work when using a public wireless network.

**5 – Always backup your data**

Get into the habit of [backing up your data](https://blog.mailfence.com/top-5-tips-to-backup-your-data/) to protect it from any kind of risk. This is probably the best tip of all for protecting your personal information online, since you’ll be able to recover it if you lose access to your data.

As a rule of thumb, you should backup all your data regularly (every week, for instance). Create at least 2 copies, both encrypted. One shoud be kept in an external hard-drive (disconnected from any network) and the other should be transfered on a secure cloud service. This way, if your external hard-drive crashes, is stolen or destroyed, the data stored on the cloud will remain safe.

**6 – Update all your software whenever you’re notified to do so**

Install updates for all your software as soon as you receive a notification. Updates often contain security patches to fix flaws in the software. These flaws could allow hackers to infect your device with a virus or malware. For example, a [keylogger](https://blog.mailfence.com/protect-yourself-from-a-keylogger/)is a software that allows a hacker to know all the keys you activate on your keyboard when you type… It’s handy for him to access your passwords and other data such as your bank account number! Don’t compromise your data security by failing to follow this easy-to-apply tip.

**7 – Use two-factor authentication (2FA) whenever it is offered**

Yes, it’s true… [2FA](https://mailfence.com/en/two-factor-authentication.jsp) implies [setting up a second authentication method](https://blog.mailfence.com/harden-mailfence-account/) (in addition to log in with your ID and password), usually typing a code sent on your phone by the website you want to connect to to prove you’re actually the user you pretend to be. And having to wait for the text message containing the code to confirm your identity is sometimes annoying. But this little inconvenience is nothing compared to what awaits you if someone manages to get hold of your email or bank accounts passwords. This tip requires a little patience to keep your sensitive data safe, but it is definitely a small price to pay. Plus, it’s quite [easy to set up](https://kb.mailfence.com/kb/setup-2fa/).

**8 – Use antivirus software on all your devices**

Virus, worms, trojan horses, spyware, [keylogger](https://blog.mailfence.com/protect-yourself-from-a-keylogger/), [ransomware](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/), … The list of different types of malware is already long, and it is likely to continue growing while you read this. And all these programs have only one target: your data! To protect your personal information and your privacy, it is therefore critical to install antivirus software on ALL your devices, including your smartphone. But beware: for the protection provided by your antivirus to be really effective, it is necessary to update it regularly. This way, it will constantly integrate the most freshly discovered malware.

**9 – Use passphrases instead of passwords**

The longer a [password](https://blog.mailfence.com/bad-password-habits/) is, the more difficult it is for a hacker to discover it and ruin your personal information safety. The ideal is therefore to use a sequence of words or a phrase to obtain a very long password. For you, it will only be a phrase to remember. The title of your favourite song? The advertising slogan you find the most absurd? The motto that inspires you the most? You choose! Any of them will do, provided you don’t re-use a password you already have picked for another website (all passwords must be unique). Also, if it’s not already the case, use a password manager (LastPass, Biwarden, Keeper) to store your passwords in safety. There are plenty of [password best practices](https://blog.mailfence.com/password-best-practices) you might want to use.

**10 – Manage cautiously your privacy settings**

Most apps allow you to determine your privacy settings preferences, and you should always chose the more private option. Never forget that all your apps are constantly collecting data about you. Why do they collect all this data? Probably to sell it to the highest bidder… who will use it to build a profile of you to be even more persuasive to sell you their stuff. If you want to protect your privacy, protect your data from this systematic collection.

**11 – Don’t disclose any personal details**

When someone asks you for personal information by email, phone or SMS, think about it carefully before answering the message. Are you sure that the person you are talking to is who they say they are? Most organizations that might need this information already know about it, or have as a rule never to ask it to you. It could be a fraudulous attempt to get some of your information as part of a [pretexting attack](https://blog.mailfence.com/pretexting/) or a [quid pro quo attack](https://blog.mailfence.com/quid-pro-quo-attacks/).

If the request seems justified, respond to the message with this company’s email address, phone number (found on their website), or by logging onto this organization official website. Also, never keep any unencrypted file containing personal data on your computer or your smartphone. It would be easy for a hacker to get it and steal your data. Check our [email security and privacy awareness course](https://blog.mailfence.com/email-security-and-privacy-course/) to discover all our tips against [Social Engineering.](https://blog.mailfence.com/what-is-social-engineering/)

**Protect your device:**

Protecting your device is the second and most important step. Therefore, you need to understand that your device is the gateway to your digital life. The more secure it is, the more effective your defense measures will be.

**How to protect your computer and/or your smartphone or tablet from hackers**

First, we’d like to stress the importance of the**physical security** of your devices. Lock your computer or smartphone when you don’t use it! Needless to say, the first step to protecting your device is to never leave it unattended. Also, disable **lock-screen notifications and Bluetooth**. Thieves could use them to intrude into your device’s system. Protecting your device against physical theft is equally important as our following tips.

**#1 Connect to a Secure Network**

Being connected to the Internet could give attackers access to your computer. So make sure to connect to all the websites using [SSL/TLS](https://web.archive.org/web/20210618235208/https:/en.wikipedia.org/wiki/Transport_Layer_Security), and harden the devices that come with overly permissive factory-default configurations e.g., IoT devices, routers, etc. – and be sure to **secure**them.

**#2 Enable and Configure a Firewall**

A [firewall](https://en.wikipedia.org/wiki/Firewall_(computing)) is a device that controls the flow of information between your computer and the Internet, similar to a router. It prevents the disclosure of your personal data by creating a **gateway**. It will also **warn**you in case malicious individuals try to break into your computer system.

Most operating systems include a built-in firewall (Windows and macOS have theirs), as do the majority of home routers. This means you shouldn’t have to worry about setting up one, as your device is already protected. But you can **strengthen**your computer security by creating [a strong password](https://blog.mailfence.com/fr/11-bonnes-habitudes-mots-de-passe-proteger-comptes/) that will lock your firewall against any attempt to disable it (Check your Wi-Fi operator guidelines for more information).

**#3 Use**[**Antivirus**](https://en.wikipedia.org/wiki/Antivirus_software)**and Antispyware**

Installing **antivirus**and keeping it**up to date** is a critical step in protecting your computer. Likewise, install an antivirus app on your phone. Be sure to keep them updated.

But antivirus is not a magic tool capable of erasing all threats. In fact, this software is based on a **database of already known malware**, listed in an internal registry (most often, antivirus updates aim to add new entries – i.e. newly discovered viruses – to this registry).

This means that they are unable to recognize a brand-new malware. So bear in mind, using an antivirus is not a silver bullet. It will not exempt you from applying other preventive measures.

Spyware is a malevolent software designed to **monitor your employees’ activities** on their computers to gather clues helpful to steal data. The software aims to [spy on the company](https://blog.mailfence.com/why-companies-should-protect-data-from-spying/) to obtain important secret information such as patents or contracts.

Most big cybersecurity brands’ antivirus tools usually embed anti spyware. If it’s not the case with yours, get one to prevent hackers from stealing information.

**#4 Remove Unnecessary Software**

Intruders can attack your computer by exploiting software vulnerabilities. Consequently, **the less software you have, the less vulnerable your computer will be**. Therefore, remove any unnecessary software after confirming that it’s safe to remove. Likewise, disable non-essential services and cancel unnecessary default features to eliminate several opportunities for attack.

**#5 Follow the PoLP (Principle of Least Privilege)**

In most instances of a [malware infection](https://en.wikipedia.org/wiki/Malware), the malware can operate only under the rights of the logged-in user.

To protect your device and minimize the impact the malware can have if it successfully infects your computer, consider having **two kinds of user accounts** :

* A **standard**account with the minimum of features for day-to-day activities;
* An **admin**one with full operating privileges on the system you’ll log in to when you need to install or remove software or change system settings on your computer.

**#6 Use a Secure Web Browser**

[Web browsers](https://en.wikipedia.org/wiki/Web_browser) installed on new computers usually don’t have**secure default settings**. Therefore, securing your **browser**is a critical step in improving your computer’s security as more and more attacks take advantage of web browsers. Make sure you use a trusted one (why not [DuckDuckgo](https://blog.mailfence.com/how-to-degoogle/)?) and avoid unnecessary plugins/add-ons.

**#7 Update often**

Most software vendors release updates to patch or fix [software vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability), flaws, and weaknesses (bugs) in their software. And very often, the hacking of the software exposes these flaws. To prevent hacking, it is therefore crucial to download updates **as soon as possible.**

Vulnerabilities can also be present in the firmware. A firmware is a utility software designed to provide secondary functionalities to your devices (such as allowing your device to connect to any type of printer, or to support a microphone or headphones).

Enable **automatic updates**whenever possible, so that you won’t have to think about it.

**#8 Use**[**Security Best Practices**](https://blog.mailfence.com/email-security-10-best-practices/)

* **Only create strong and unique passwords**  
  The password is the first defence line against intrusions, and is also the least expensive tool to protect your device and the easiest to set up. But this will be effective only if you follow a**few basic rules**. For more tips on passwords, you can read [this article on password best practices](https://blog.mailfence.com/password-best-practices/).
* **Beware of phishing and ransomware attacks**  
  **Education**is the best defence to protect your computer and your phone against phishing or [ransomware](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/) attacks and to stop hackers on your computer. Read our articles about [Social Engineering](https://blog.mailfence.com/what-is-social-engineering/) ([phishing](https://blog.mailfence.com/what-is-phishing/), [spear phishing](https://blog.mailfence.com/distinguish-spear-phishing-from-phishing/), [whaling](https://blog.mailfence.com/social-engineering-what-is-whaling-attack/), [smishing](https://blog.mailfence.com/social-engineering-smishing/), and [vishing](https://blog.mailfence.com/vishing/)) and learn how to recognize and avoid these techniques. Follow our [Email security and privacy awareness course](https://blog.mailfence.com/email-security-and-privacy-course/) and spread the word!
* **Use two-factor authentication**  
  Two-factor authentication (or [2FA](https://kb.mailfence.com/kb/setup-2fa/)) works as a**second layer of protection**after your password. Many websites will offer to use it to secure your account and restrict its access to you. Sure, 2FA adds some delay to your connection, but the benefits are enormous.

**#9 Do Not Use Illegal Software**

It might [compromise your data](https://blog.mailfence.com/protect-yourself-from-a-keylogger/) and your computer **security**, and even break the law.

**#10 Have a Backup**

Use [backup](https://blog.mailfence.com/top-5-tips-to-backup-your-data/)software to [**schedule**](https://blog.mailfence.com/secure-online-mailfence-calendar/)many backups a week, depending on your volume of computing activities. Include all devices and software you use in your backup perimeter, and make at least **two copies** :

* The first one on an external hard drive (hard disk, USB key, NAS…) ;
* A second one on a cloud storage platform

Ideally, you could add a**third one**on another external hard drive to be**stored externally**to protect your files from any disaster that may affect your home or company.

**If it’s too sensitive, avoid keeping it in your device**.

**Additional tips to protect your computer and other devices**

**#11 Elaborate your Disaster Recovery Plan**

What would you do if your company was hit by a disaster tomorrow morning (consider a fire or ransomware intrusion)? Are you ready for this kind of scenario? Do you accurately know what you would have to do to **prevent more damage** and **restart your business** despite the loss of data or destruction of equipment?

If you’re unsure about the answer to this serious question, consider elaborating your own**disaster recovery plan**. In the middle of the chaos, you’ll be grateful to have a**to-do list**to contain the risks, remedy the damage, and reactivate what can be restored.

Designing this type of program is not something that can be improvised, and you may need the help of an IT specialist to set it up and test its validity.

**#12 Encrypt your data**

[Encryption](https://blog.mailfence.com/symmetric-vs-asymmetric-encryption/) scrambles data and messages, usually using a mathematical key. To get back a readable **data or message**, the user will need to know this key to decipher it. This system makes all data safe because they become unreadable, meaning they remain **private**. It’s an effective way to prevent interception for espionage purposes and data theft.

You can also encrypt your **web traffic**using a [Virtual private networks (VPN)](https://blog.mailfence.com/vpn-secure-email/). It will encrypt your data before its transmission so that nobody can read it during its transit. The relevant data will only be deciphered at its destination (the website/software you’re communicating with).

Also, a website using [SSL/TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) will encrypt the data you exchange with it, so that malicious individuals cannot intercept it. You can recognize these websites thanks to the padlock they display in your browser’s search bar when you’re connected to them. Ensure to be connected to the **secure** version of a website by activating the [HTTPS Everywhere](https://www.eff.org/https-everywhere/faq) extension. It will redirect you seamlessly to the SSL-secured version of a website if it exists.

**Bad Password Habits:**

Following good password habits is a key factor in making all of your online and offline defenses stronger. There certainly are password managers, that do a great job. However, avoiding bad password habits is something that you should do yourself.

**Less than 1 second : that’s how long it will take for a fairly savvy hacker to crack the password “qazwsxedc”. So, more than ever, you need to avoid bad password habits to secure all your accounts online. To help you to spot them, we’ve compiled a list of bad password habits.**

Unfortunately, [2021 statistics](https://www.popularmechanics.com/technology/security/a38305276/worst-passwords-2021/) show that “123456” was once again the leader in the list of the most common passwords used worldwide. Needless to say, if it requests less than 1 second to guess “qazwsxedc”, it will be even easier to compromise all accounts hiding behind this other example bad password. But what are the practices to avoid when it comes to passwords ?

**A list of bad password habits**

**1 – Using the same password everywhere**

Analysts estimate that some 50% of people on the Internet are still using the same password for all of their logins. This is one of the riskiest things you can do online. Because it’s only a matter of time before one of your online accounts gets compromised.

And if you use the same keyword across multiple websites, just one website leak will allow a hacker to access to many of your other online accounts. It could be an online store where you have entered your credit card information, your Paypal account, or any other account associated with your money.

Or alternatively, the cyber pirate would be able to reach an account on which you have entered particularly sensitive confidential information. Access to one of your accounts could also allow them to impersonate you and post hate messages on social networks to damage your reputation.

**2 – Never updating passwords**

When was the last time you updated one of your passwords? If you have never done it yet, this is the time to do it. It could be useful to change your password, for example, every once a year, to avoid your account compromises if respective service provider is breached but is not yet aware of it (this practice is only useful if you set a long and complex password with no parts or variations of old password).”

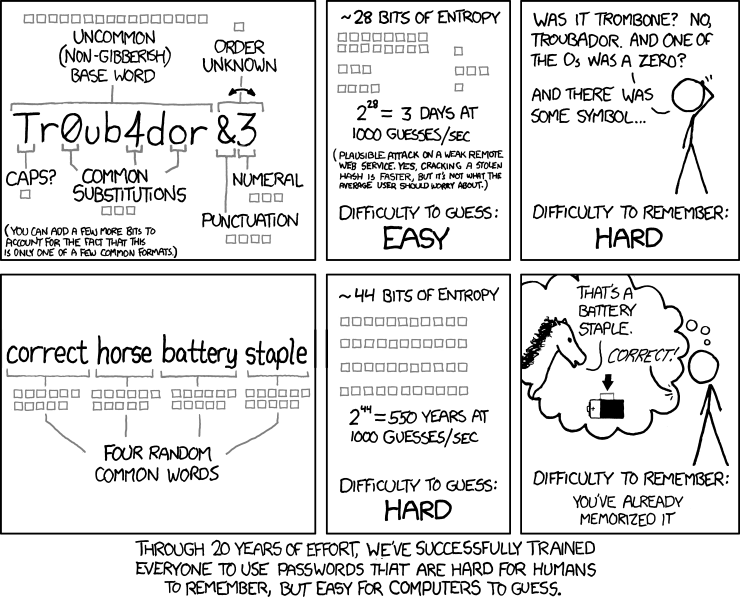
**3 – Having too short passwords**

Short passwords are easier to guess using brute forcing. It consists of trying all possible combinations of letters until you find the right one. And don’t think that this boring job puts off hackers: they can rely on software to do the job for them!

Avoid using too common passwords. Even better, use passphrases instead. Indeed, they’re longer and easier to remember.

So don’t do what most people do and refrain from using one of the 200 most commonly used passwords (which are also the worst ones). Also, never use an understandable word (“Dolphin”) or expression (“ILoveYou” or “Ferrari”) : Hackers’ cracking tools are designed to recognize them.

Instead, pick [random expressions](https://blog.mailfence.com/password-best-practices/), combine them with uppercase and lowercase letters, and special symbols such as @ and numbers to create a complex password. Avoid replacing letters with similar symbols or numbers (5 instead of s, or @ instead of a) in an actual word or expression, because their software is programmed to spot them too.

Source: https://xkcd.com/936/

**4 – Storing passwords in the browser**

Yes, having all your passwords in your browser is convenient and allows you to connect faster to all your online accounts. But your browser is not a secure place for them.

First, because most often, you’re connected to them by default. Which means anyone having access to your [computer](https://blog.mailfence.com/10-tips-to-protect-your-computer/), phone or tablet (when it’s stolen, or hacked) will be too.

And secondly, because the browser’s owner is more likely to have prioritized [your user experience](https://blog.mailfence.com/how-to-degoogle/) when designing it to convince you to stay with them at all costs and not [your data security](https://blog.mailfence.com/tips-on-how-to-protect-your-data/). So that any vulnerability in the browser/browser extension (plugins/add-on’s) can lead to compromising browser password managers.

It’s far better to use a [password manager](https://en.wikipedia.org/wiki/Password_manager) instead. The bonus is that password managers comprise many useful features, such as a password generator to help you create strong and unique passwords.

The same goes for the “remember me” option some websites offer. Here again, it will be very easy for any thief or cyber pirate having access to your computer, phone or tablet to log in this website and do whatever they want to do.

**5 – Sharing passwords too freely**

Every one of us had to share one or two passwords at some point with someone else, whether to allow their guests to get their wi-fi at home, their kids to watch a movie on their Netflix account, or a colleague to use software in their company. But ideally, you should not do this frequently and only with people you trust.

Even better, you should change this password as soon as this person does not need it anymore.

If you really need to share a password with someone, use a secure way to do it.

How do you communicate a password to someone else that is not in front of you? Email, instant chat, or SMS may seem the perfect way to accomplish this task. The recipient can even copy and paste the password directly to log in!

Unfortunately, if it is easy for your recipient, it must also be easy for the hacker who managed to intercept your message… So it’s not the best thing to do.

A better idea is to send the message in two steps (ideally on two different media: an email and an SMS, for example).

**The Top 10 list of worst passwords examples**

As we’ve already seen, once again, 123456 was 2021’s most used password… And it was closely followed by… 123456789. Here is the Top 10 of most common passwords [compiled by NordPass](https://nordpass.com/fr/most-common-passwords-list/), and as you can see, according to our point 2, all are terrible ones :

* 123456
* 123456789
* 12345
* qwerty
* password
* 12345678
* 111111
* 123123
* 1234567890
* 1234567

And the [list goes on and on](https://nordpass.com/fr/most-common-passwords-list/), with “888888” at the 59th position, “1111111111” at the 114th one, and “444444” at the 199th.

* [11 Password Best Practices](https://blog.mailfence.com/password-best-practices/)– 7 min read

Once you drop bad password habits you’ve been making, here are 11 best practices to adopt to ensure your passwords are strong.

**How well do you remember your passwords? If you’re like most people, you probably keep forgetting passwords. You might be guilty of reusing the same password on different accounts, or creating weak passwords.**

**In this article, we’ll go over 11 password best practices that you should start implementing now to not only be able to create stronger passwords, but also remember them more easily and keep them secure.**

**Lose the Bad Habits First**

Humans are, for the most part, creatures of habit. Unfortunately, those habits are often bad and when it comes to bad password habits, these can drastically compromise your online security.

A lot of us are guilty of at least one, if not all of these [top 5 bad password habits](https://blog.mailfence.com/bad-password-habits/):

* **Reusing passwords**
* **Not updating their passwords**
* **Using short passwords**
* **Storing their passwords in the browser**
* **Sharing passwords**

You seriously need to ditch these today. Instead, here are 11 password best practices that you should be doing:

**Password Best Practices:**

**1. Use longer passwords**

While using a 5-character password may be easier to remember, it’s also much easier to crack than a password that has 10+ characters.

According to the [National Institute of Standards and Technology](https://www.nist.gov/) (NIST) guidelines, the minimum length for user-generated passwords should be 8 characters, though even this can be too short, depending on what they are protecting and who is trying to breach it.

For example, penetration testers at [LMG Security](https://www.lmgsecurity.com/how-long-should-your-password-be-a-technical-guide-to-a-safe-password-length-policy/) were able to crack any 8-character Microsoft NT LAN Manager password hash in under 8 hours, while it would take them around 8 years for 10 characters, 77,000 for 12, 710,5 million years for 14, and 6.5 trillion years for a 16 character password hash.

**2. Make your passwords more complex**

Of course, if your password only contains one type of character, like lowercase letters, it will still be vulnerable to a simple dictionary attack.

The solution here is to not rely on just letters, but also to make your passwords more complex using a combination of lowercase and uppercase letters, numbers and special characters.

For instance, you can take a word, like “password”, which has 8 characters, so it fits the NIST guidelines and replace some of the letters with other symbols like this: “P@55w0rd”. Now you have uppercase letters (P), special symbols (@), numbers (55 and 0) and lowercase letters (r and d), which should make the password a little harder to crack.

**3. Update your passwords**

Given enough time and resources, any password can be cracked eventually.

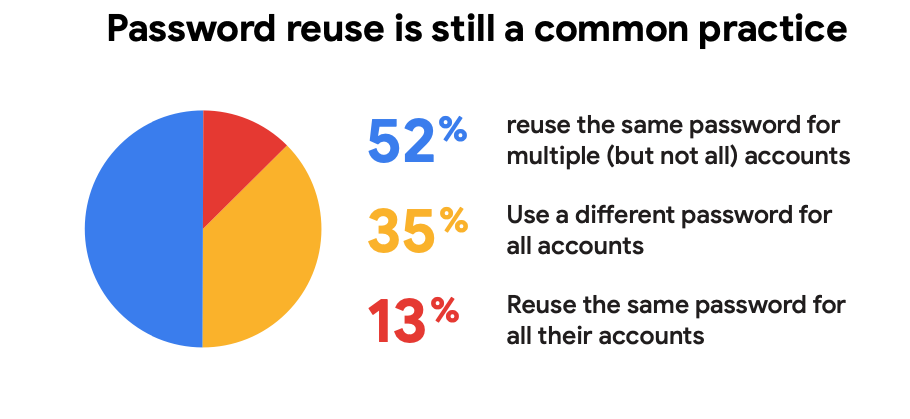
As such, password security often becomes a game in which you constantly need to be one step ahead of the hacker and that means changing your passwords from time to time.

For a long time, the recommended frequency for password changes was 1-3 months. This, however, creates an additional problem. The more often the user is prompted to change their password or update it, the more likely they will simply use the same password, only slightly changed. This, ultimately, solves nothing.

[NordPass](https://nordpass.com/blog/how-often-should-you-change-passwords/), for example, recommends that you change passwords every year, saying:

Finally, there actually is a good period of time after which you should change your password: one year or so. It’s a good amount of time that lies neatly between being just short enough that you aren’t feeling forced to make a new password (and therefore a bad one) and just enough that you might start considering it a risk to your account security, especially to things like ransomware or a [pharming](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/) attack.

**4. Don’t reuse passwords**



A [2019 joint study by Google and Harris Poll](https://services.google.com/fh/files/blogs/google_security_infographic.pdf) fully revealed just how common practice is password reuse.

According to the study, 52% of 3,000 U.S. respondents (16 to 50+ years) said they reuse the password on several (but not all) their accounts, 35% use a different password each time and 13% reuse the same password on all of their accounts.

Even if you are reusing the password on just two accounts, that’s pretty much doubling the chance of either ending up under the hacker’s control should any of the two accounts become compromised following a data breach.

Every account that you own should have a unique password to mitigate the threat of a data breach on one account affecting your other accounts.

**5. Use Two-factor Authentication (2FA)**

Relying on passwords as the sole account security is not enough as even the best one can be compromised, cracked, or leaked.

This is where [Two-factor authentication](https://kb.mailfence.com/kb/setup-2fa/) or 2FA comes in.

2FA creates an additional verification method on top of the password. This can be a token, SMS message, fingerprint scan or something else that the user receives on another device they own. This way, the logic is that, even if someone manages to get your password, they wouldn’t be able to do anything without knowing the second verification method.

**6. Don’t let the browser save your passwords**

If you’re visiting a website for the first time and creating a password, your Internet browser will ask you to allow it to store your password.

While this sounds like a good idea on paper, it really isn’t. For companies that develop browsers, like Google or Mozilla, the primary focus isn’t on the security of their customers, but on usability and getting more customers. That’s why your passwords won’t be safe with them.

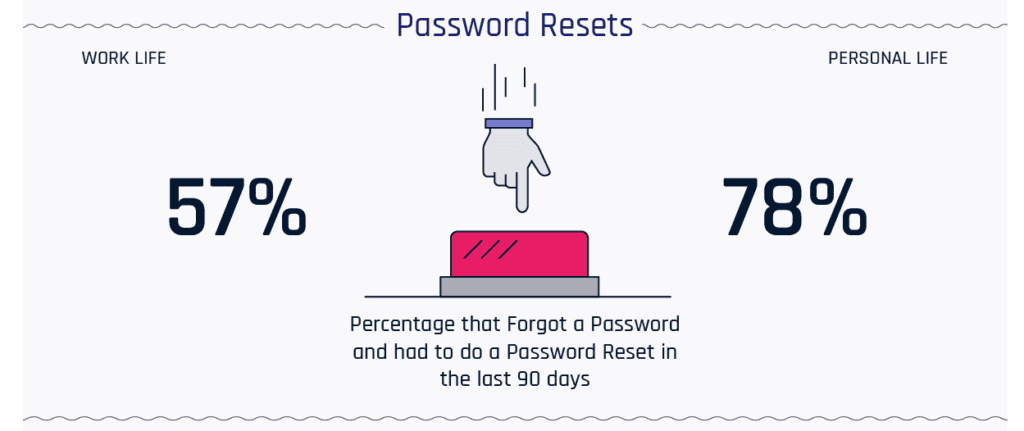
Don’t worry about needing to remember all your passwords. The next best practice is the solution.

**7. Use a password manager to keep track and store your passwords**

A study by NordPass from 2020 revealed that the average person has 100 passwords.

Naturally, remembering all these passwords would be incredibly difficult, which means forgetting passwords way too often and resorting to resetting passwords.

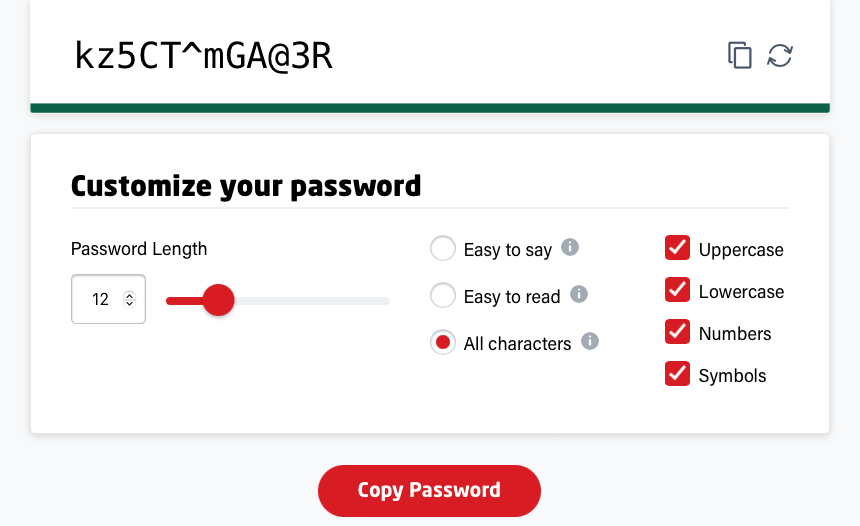
A study by [HYPR](https://blog.hypr.com/hypr-password-study-findings) from 2019, found that 78% of people had to reset a password they couldn’t remember in the last three months.



Luckily, there is an easy solution for storing passwords safely and making sure you never forget them – password managers, like NordPass, which we already mentioned.

However, don’t rely too much on password managers, as they can still be vulnerable to data breaches. This happened with LastPass in 2015, for example.

**8. Randomize your passwords**



Taking a common word and then replacing the letters with other symbols will make your password harder to figure out, but there’s an even better password best practice.

Using a password generator.

Every password manager also includes a generator that you can use to create secure and random passwords.

For example, with the LastPass Password Generator, you can set the password length up to 50 characters, use uppercase, lowercase, numbers and symbols, or choose a password that’s easy to say (avoids numbers and special characters, easy to read (avoids characters that can be mistaken for one another like 0 and O) or use all characters.

**9. Check the security of your credentials**

Often, what seems to us like a strong password, turns out not to be that strong at all and is easy to crack.

This is why you need to check your password strength from time to time. One tool that you can use for this is [Kaspersky Password Checker](https://password.kaspersky.com/).

All you need to do here is enter your password in the field and the checker will tell you how secure (or not secure) your password really is.

Another tool that you can use to check your account security is [Have I been Pwned](https://haveibeenpwned.com/). This page lets you enter your email address to see if it has been found in any data breaches.

**10. Salt & hash passwords**

Another password best practice that NIST recommends is to use salt and hashing on your passwords.

In this case, first a random string of characters is added to the password (salt), before hashing the password. This adds another layer of security to the password and it becomes impossible for a hacker to break the password by reversing the hash.

**11. Limit failed password attempts**

People will often mistype passwords, but it makes no sense for a website to lock them out of their account after the first failed attempt.

Still, they also shouldn’t give a potential hacker too many opportunities to figure out the password.

The number of failed login attempts that you should allow is, of course, difficult to set, as it largely depends on your organization’s security risk level. For example, [Microsoft recommends 10](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold) as a good starting point before a lock.

**Social Engineering: Overview with examples**

Humans are considered as the weakest link in any sort of defense. The thing that makes us vulnerable is the tendency to trust someone or something based on certain criteria. This section will briefly go through different kinds of social engineering.

Social engineering are a group of techniques that cybercriminals use that exploit the human nature and trick people to do something that will weaken their security.

If you’re like most people, you probably don’t know much about social engineering attacks. Or do you believe it only aims to dupe unsuspecting victims to steal some money?

**You may not realize that social engineering techniques can take many forms. And anyone can fall victim to one – even you.**

In this guide, we will cover everything you need to know about social engineering attacks, including:

* what a social engineering attack is;
* the different forms a social engineering attack can take;
* how to quickly detect a social engineering attack;
* and most importantly, how to avoid falling victim to one!

So without further ado, let’s explore!

**What is Social Engineering?**

**Social engineering gathers many techniques to exploit our human nature to induce behaviors and mistakes that will lead to weakened security.**

It will allow cybercriminals to access information, money or control what they’re looking for. It’s not a unique kind of attack but rather a group of different scams that share several similarities:

* Scammers attempt to obtain sensitive information or money;
* They exploit trust and human behavior to manipulate their victims and achieve their goals;
* They exploit their victims’ lack of knowledge and their inability to implement security measures to protect themselves;
* Their schemes often involve using personal information (identity theft) to appear more authentic.

Remember the ancient Greeks’ “gift” horse to the city of Troy? An excellent real-world example.

**At the heart of every social engineering attack lies *manipulation.***

Forget about brute force tactics. With social engineering, attackers use manipulative tactics to lead their victims into compromising themselves or the security measures they rely on. Scammers connect with their victims to infuse confidence and influence their actions.

**As attackers become more familiar with their targets’ motivations, they can craft persuasive tactics to lure them into potentially destructive behavior.**

And it works: many cybersecurity incidents are successful social engineering schemes carried out by external attackers. They play with human weakness to make their victims unwittingly provide access to sensitive information or money.

**How Do Social Engineering Attacks Work?**

As we already mentioned, social engineering relies on manipulation. It can take on various forms (as we’ll explore later).

However, every social engineering attack will exploit one of the following human traits.

**Trust**

The hacker will send a message [spoofing](https://blog.mailfence.com/email-spoofing/) an organization’s communication codes, such as its logo and other brand features (fonts, writing style, etc.).

They want to trick the victim into doing things they would routinely do with this specific organization (click on a link, download a file, etc.) because they trust it and just don’t challenge the message’s origin.

**Compliance with the authority**

Obedience to authority is another human trait social engineering tactics can exploit.

Pirates will impersonate a high-ranking individual or a government agency to induce their obedient target to do something.

**Sense of urgency and/or fear**

People often act without thinking when faced with a sudden sense of panic.

They are vulnerable to social engineering scams that prey on such emotions. These deceptive tactics leverage fear and urgency in various ways:

* false credit card alerts;
* virus warnings;
* exploiting one’s [FOMO](https://www.spiceworks.com/it-security/vulnerability-management/guest-article/phishing-dont-let-fomo-kick-you-into-a-fifa-world-cup-scam/) (fear of missing out).

The panicking victim is lured into taking action without taking the time to consider the implications of their actions. Often, under stress, they will forget to double-check the request’s legitimacy.

**Greed**

You wouldn’t refuse a gift, would you? Scammers understand this.

**This is why many scams leverage our greed to attract us with money rewards, free iPhones and other prizes.**

Ever heard of the “unexpected inheritance” scam? This is a classic phishing attack promising you a large sum of money from a distant relative or a wealthy benefactor. The money is supposedly blocked for some obscure reason… All you need to do is pay the administrative fees to get the money.

Sound too good to be true? That’s because it is! This is a perfect example of a scam using our attraction to money, gifts, or easy rewards.

**Generosity**

Finally, our generosity is often exploited in social engineering attacks.

Attackers exploit generosity by researching social media to find out what matters to you and impersonating organizations linked to your causes. For example, they might pose as a charity you support to solicit donations.

**Social Engineering Attacks: What Do They Look Like?**

There are many kinds of social engineering attacks with subtle varieties. Here are some of the most common ones.

[Phishing](https://blog.mailfence.com/what-is-phishing/) scams are the most common types of social engineering attacks used today. Phishing scams rely on emails to make a connection with the target. Other specific types of phishing attacks exist such as:

* [smishing,](https://blog.mailfence.com/social-engineering-smishing/) a phishing attack that relies on SMS;
* [vishing](https://blog.mailfence.com/vishing/) which relies on actual phone conversations;
* [spear phishing](https://blog.mailfence.com/distinguish-spear-phishing-from-phishing/) which targets specific individuals with personal information to make it appear legitimate;
* [whaling attacks](https://blog.mailfence.com/social-engineering-what-is-whaling-attack/) which are phishing attacks that target high-ranking executives.

[Pretexting](https://blog.mailfence.com/pretexting/) is another form of social engineering where attackers focus on creating a plausible pretext, or a fabricated scenario, that they can use to steal their victims’ personal information.

[Baiting](https://blog.mailfence.com/what-is-baiting-in-social-engineering/) is, in many ways, similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that hackers use to entice victims, just like the Trojan horse.

Similarly, [quid pro quo attacks](https://blog.mailfence.com/quid-pro-quo-attacks/) promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good.

[Scareware](https://blog.mailfence.com/social-engineering-what-is-scareware/) aims to make its victims believe a virus infected their device, and they need to buy or download specific software to fix it.

Watering Hole Attacks happen when attackers compromise a website frequented by a specific group of users. When these users visit the site, their devices are infected with malware.

A Honey Trap is when attackers create fake social media profiles to befriend targets and extract confidential information through deceptive relationships.

Finally, Reverse Social Engineering creates a situation where the victim seeks help, allowing the attacker to pose as a helper and extract sensitive information.

**Physical phishing attacks**

Phishing attacks can also happen in the “real”, physical world.

The most common form is called “[shoulder surfing](https://blog.mailfence.com/social-engineering-what-is-shoulder-surfing/)“. This is when someone observes directly over your shoulder to gain information such as passwords or PINs after luring them into doing an action necessitating credentials.

Another social engineering attack type is [tailgating](https://blog.mailfence.com/what-is-tailgating/), where someone seeks physical entry to a restricted area where they are not allowed to be.

**Common characteristics of social engineering attacks**

Most of these social engineering attacks share the following characteristics:

* **Personal information:** attackers seek information such as names, addresses, and social security numbers.
* **Link shorteners or embedded links:** these links actually redirect users to suspicious websites in URLs that appear legitimate.
* **Malware:** social engineering can also be used to set up malware either on top of stealing the victim’s credentials or with the sole purpose of compromising the victim’s device.

**Social Engineering Attacks: How to Stay Safe?**

Now that we’ve identified the different forms of social engineering and their characteristics, let’s talk about how to avoid them!

What follows are various steps you should take to identify social engineering attacks, and protect yourself from future ones.

**#1: Take your time to evaluate the situation**

Take the time to consider the whole situation and examine the message carefully, even if it is quite worrying.

* Is this message unexpected?
* Does it originate from where it’s supposed to?
* Ensure you are interacting with trusted contacts by confirming their identity. Whenever possible, contact your sender directly to make sure they sent what was received.
* Also, check for spelling mistakes, oddities in the logo, or other revealing details. Does this organization usually communicate in this manner?
* Again, in case of any doubt, take your phone and call the official number or the number you’re used to call (and not the provided number) to get more information.

**#2: Check the URL or file before clicking**

Never, ever click on an attachment or link in email without double-checking.

**Any attachment in a message can hide a virus or some other kind of malware, such as**[**ransomware**](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/)**.**

**A link in a message can lead you to a staged website set up to steal your data or infect your device with**[**malware**](https://blog.mailfence.com/10-tips-to-protect-your-computer/)**.**

Before clicking on them, inspect them carefully:

* Is there any message or a prompt indicating the attached file contains macros? If yes, make sure you don’t enable macros to view the file.
* Were you expecting this file or link?
* In doubt, don’t hesitate to check and ask the sender directly if it’s coming from them (contact them with your usual means of contact).
* If in doubt, DO NOT click! Ask a colleague, friend, or family member if you are unsure. Or refer to an IT expert if you don’t feel comfortable assessing the situation.

**#3: Be aware of your valuables**

Even if you’re not a millionaire, you own many things that could arouse the greed of cybercriminals:

* your data (which can be sold on the dark net);
* software access you have in the company you work for;
* detailed social network accounts, with numerous pictures, and comments revealing what you like, what you support, etc.. This means it will be straightforward to profile you and determine the appropriate strategy to target you. Therefore, be careful with what you share on social media.

Take the time to look at your privileges, communications on the net, and try to understand the potential you offer for any scammer. Being more aware of this can improve your ability to detect social engineering attacks.

**#4: Learn about social engineering scams**

Congratulations! Just by reading this guide, you’ve already made yourself less vulnerable to social engineering attacks. **Education is key to avoiding social engineering attacks.**

As individuals, we are in most cases at the origin of a potential attack due to our lack of awareness and knowledge.

**#5: Use security software to avoid spam and phishing emails**

To protect your device and your data from cyberthreats and intrusion attempts, you must use an antivirus and make [periodic backups](https://blog.mailfence.com/10-tips-to-protect-your-computer/).

**But you must also use a**[**secure email solution**](https://blog.mailfence.com/secure-email-and-end-to-end-encryption/)**to ensure messages coming into your inbox don’t include any malware or any malicious part, and to block them if that’s the case.**

Emails are one of the most common gateways for hackers. So make sure you have [MFA activated](https://mailfence.com/en/two-factor-authentication.jsp), and get accustomed to sending [encrypted emails](https://blog.mailfence.com/secure-email-and-end-to-end-encryption/) that are [digitally signed](https://blog.mailfence.com/how-do-digital-signatures-work/).

**#6: Avoid single points of failure**

A [single point of failure](https://avinetworks.com/glossary/single-point-of-failure/) is a common term used to describe having all your eggs in one basket. If that point gets breached, all your data is compromised. This is why you should avoid connecting all your accounts with Facebook or Gmail.

The more intertwined and dependent your accounts are, the more damage a security breach can cause you.

**#7: Unique logins and secure passwords**

Linked to #6, use different logins for each service and [strong, unique passwords](https://blog.mailfence.com/bad-password-habits/). Consider using [email aliases](https://kb.mailfence.com/kb/what-is-the-difference-between-an-alias-and-a-mailbox/) and [password managers](https://blog.mailfence.com/bad-password-habits/) to manage your credentials.

**#8: Get creative with security questions**

This one might sound trivial. But the additional security questions websites ask you are to, usually, set up a 2-step verification (2SV) security measure.

So be creative and avoid easily guessed answers such as your date or place of birth. A hacker will find those in a few minutes. Also, do not confuse 2SV with Multi-Factor Authentication (MFA) or TFA which we strongly suggest you set up anyway.

**#9: Use credit cards wisely**

If you use a debit card and a hacker gets access to the number, your entire bank account could be drained. You can further secure your credit card by not storing card numbers on websites or [using disposable or virtual card numbers](https://www.capitalone.com/learn-grow/money-management/what-are-virtual-card-numbers/) (offered by Citibank, Bank of America, and Discover).

**#10: Frequently monitor your accounts**

[Be on the lookout](https://blog.mailfence.com/harden-mailfence-account/) for both identity theft and credit card fraud. Regularly check in with your account balances and credit score.

**Types of Social Engineering**

**Tailgating:**

Tailgating (piggybacking) is a social engineering technique in which one tries to enter an area they are normally not allowed to go in, usually be following someone closely behind.

Basically, tailgating definition is when someone sneaks into a restricted area by using someone else. This can be by following someone real close carrying something and asking them to “Hold the door please!”. Or, an attacker can fool people by pretending to be someone else, just like [phishing](https://blog.mailfence.com/what-is-phishing/) or [pretexting](https://blog.mailfence.com/pretexting/) (for instance a pest exterminator)

Tailgating is different from other Social Engineering attacks, though. Indeed, it is a physical intrusion, in order to access sensitive data, money, …. This way, it’s closer to [baiting](https://blog.mailfence.com/what-is-baiting-in-social-engineering/).

A person impersonates a delivery driver and waits outside a building. When an employee gains security’s approval and opens their door, the attacker asks that the employee ‘hold the door’. Thereby gains access to the company through an authorized person.

The impostors can take many roles, such as repair guys, individual pretending to hold heavy boxes. Anyone that you wouldn’t think twice to hold the door to. Once inside, they can use other social engineering attacks like [shoulder surfing](https://blog.mailfence.com/social-engineering-what-is-shoulder-surfing/) to steal information from unsuspecting employees.

However, tailgating does not work in all corporate settings. For instance, in large companies, everyone entering a building need to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to pass.

The core focus of an attacker in this type of social engineering is to get physical access to the site. Entry to a restricted area, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access. Following common courtesy – the legitimate person will usually hold the door for the attacker.

The most famous tailgating attack example is probably the well-known story of [Frank Abagnale](https://en.wikipedia.org/wiki/Frank_Abagnale), whose story you have probably discovered in the movie “Catch Me If You Can”. Abagnale scammed many people and entered many restricted areas where he was not allowed. Acting with confidence made him go many places and fool many people.

**How to prevent tailgating or piggybacking in your company?**

A tailgating attack can be especially dangerous to mid-sized and larger organizations as there is too much at stake. Some examples are: stealing company secrets, money, and equipment. Another severe example is to install a backdoor to the server to eavesdrop on every conversation on the company’s network.

If you are working for a mid-sized company then you should start challenging everyone who wants to get access to the premises. It may seem rude and awkward however it is in your company’s best interest. Ask management to install biometric scanners and turnstiles to prevent a tailgater from just walking in the building.

Biometric scanners and turnstiles prevent the tailgater from walking with you inside the building as they only allow for one person at a time. Additionally, you should challenge that individual and ask questions that only employees would know.

Although it looks simple and, tailgating or piggybacking can be an effective way your competitors can use to spy against your company. Learn more about securing your company from [data spying](https://blog.mailfence.com/why-companies-should-protect-data-from-spying/) and [protecting your computers](https://blog.mailfence.com/10-tips-to-protect-your-computer/).

**Knowledge is power**

While one probably can’t waltz into a military base announcing “Exterminator!”, tailgaters often take advantage of unaware employees. It is absolutely vital that you train your employees and arm them with knowledge that will help them prevent such social engineering attacks.

You can provide them with a [free security & privacy awareness course](https://blog.mailfence.com/email-security-and-privacy-course/) to make sure they never fall for a tailgating attack again. Every time your company gets a new intern you should make sure you provide them with basic cybersecurity training, as 99% of interns are completely unaware that such attacks exist.

None of these tips will matter if you don’t stay vigilant and be suspicious of everyone you don’t know. Holding the door for a person who is “running late” seems harmless but that decision carries a lot of weight. As an employee, you are responsible for making sure that nobody except authorized personnel enter the building(s).

**The key to stand against this type of social engineering attack is to**

**KEEP YOUR EYES WIDE OPEN and STAY VIGILANT in the work-premises!**

**Quid Pro Quo Attacks:**

Sometimes bad actors can trick you into thinking they are doing you a favor that you need to return. But, no matter if you willingly give them your sensitive data or not, they can always use it to steal money and more data.

**Quid pro quo is a kind of**[**social engineering**](https://blog.mailfence.com/what-is-social-engineering/)**attack where a hacker promises a profit in exchange for information that can later be used to steal money, data, or take control of a user account on a website.**

A quid pro quo attack is characterized by a “**give and take**” exchange. It literally means [*something for something*](https://en.wikipedia.org/wiki/Social_engineering_(security)#Quid_pro_quo). This notion of exchange is crucial because as human beings, we obey the law of **psychological reciprocity**. This means that every time someone gives us something or does us a favour, we feel **obliged to return the favour**.

In the case of quid pro quo, the promised benefit or advantage in exchange for information usually takes the form of a **service**(when it takes the form of a good, it is a [baiting attack](https://blog.mailfence.com/what-is-baiting-in-social-engineering/)).

Let’s say you are contacted by an IT employee who **offers**to perform an audit on your computer to remove potential viruses that could lower your computer’s performance. But to do this, he needs your login and password. Nothing could be more natural! You provide him with this information **without any discussion**: after all, you’ve been complaining about your computer’s slowdown for months. Except that this exchange of goodwill may not be a good one, and that you may have just fallen into the **trap** of a quid pro quo attack.

Quid pro quo attacks are based on **manipulation**and **abuse of trust**. As such, they fall into the category of [social engineering techniques](https://blog.mailfence.com/what-is-social-engineering/), such as [phishing attacks](https://blog.mailfence.com/what-is-phishing/) (including [spear phishing](https://blog.mailfence.com/distinguish-spear-phishing-from-phishing/) and [whaling attacks](https://blog.mailfence.com/social-engineering-what-is-whaling-attack/)), [baiting](https://blog.mailfence.com/what-is-baiting-in-social-engineering/)or [pretexting](https://blog.mailfence.com/pretexting/).

**What is the difference between Quid Pro Quo and Pretexting?**

The [pretexting technique](https://blog.mailfence.com/pretexting/) is also a form of social engineering. But it is based on a **fairly elaborate scenario**(a good pretext) to obtain sensitive information from the victim. Often, this scenario involves the intervention of people with a specific **authority**(manager, technician, police officer, etc.) and/or implies a certain **urgency**, to force the victim to act quickly, without thinking. For example, the hackers will claim that they need to obtain some information to confirm the victim’s identity.

This scenario is more elaborate than the quid pro quo attack, and unlike the quid pro quo attack, it is not based on an **exchange**.

**What is the difference between Quid Pro Quo and Baiting?**

Like [baiting](https://blog.mailfence.com/what-is-baiting-in-social-engineering/), quid pro quo attacks are social engineering techniques. As such, both of these cyber threats rely on **psychological manipulation** and **confidence building** to obtain sensitive data from an overly trusting victim. However, in quid pro quo attacks, the hacker offers a service to his victim in exchange for sensitive information. In the case of baiting, the victim is “baited” with**irresistible offers**: a gift or a cash reward, for example.

In addition, quid pro quo attacks are often simpler than baiting attacks. And they don’t require a lot of preparation, nor sophisticated tools.

**Some examples**

One of the most common quid pro quo attacks scenarios involves **impostors**posing as an**IT employee**. The hacker contacts as many company employees as possible on their direct line to **offer**alleged IT support.

The hacker will promise to solve a problem quickly in exchange for disabling the antivirus program. Once disabled, the fake technician can install **malware**on the victims’ computers, posing as software updates.

In another common scenario, the hacker seeks to steal an employee’s credentials. Here again, the scammer will contact the employee by introducing himself as a tech specialist from an IT company specialized in troubleshooting bugs and software problems. After asking the victim a few questions to determine what problems they are having with their PC, he will **offer**to take a look at it:

No problem, I’ll fix your problems right away! All I need is your login and password!

This is a **red flag** you should be aware of!



**How to avoid Quid Pro Quo attacks**

As with other types of social engineering, you should take security measures to safeguard yourself and your sensitive data.

* Adopt a **cautious attitude**: a “gift” or “service” is never completely free. If it sounds too good to be true, it probably is! In the worst-case scenario, it is a quid pro quo attack.
* Never give personal or account information **unless you initiated the exchange**. After a possible intervention in which you have given your login details, **change your password** to prevent further use.
* When a company contacts you, call them back using the phone number listed **on their website**. Never call them back using the phone number provided by someone you have spoken with.
* If you are **unsure**about a call you received, it is wiser to leave it.
* Use [**strong passwords**](https://blog.mailfence.com/password-best-practices/) and **change**your passwords **regularly**. Review our article on passwords to [get into good habits](https://blog.mailfence.com/bad-password-habits/).
* **Train yourself** to recognize social engineering techniques and other cyberthreats. Check out our [email security and privacy awareness course](https://blog.mailfence.com/email-security-and-privacy-course/) to **educate yourself.**
* Protect your computer with these [10 tips](https://blog.mailfence.com/10-tips-to-protect-your-computer/).

**Protect your organization**

One can also use a quid pro quo attack to obtain information to launch a more dangerous attack on a **business**, such as a [phishing](https://blog.mailfence.com/what-is-phishing/) or [ransomware attack](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/). So you should not neglect this type of attack, and your company should take steps to protect itself against them:

* All of your employees must**be aware** of [cyberthreats](https://blog.mailfence.com/cyber-threats-why-pandemic-responsible/) and cybersecurity. They must be able to identify the manipulative tactics employed in quid pro quo attacks, or other kinds of [social engineering techniques](https://blog.mailfence.com/how-to-avoid-social-engineering-schemes/). They should also refrain from transmitting sensitive data via phone or email;
* Adopt **cybersecurity tools**to protect your computer systems such as a firewall and antivirus software;
* Use secure tools to store your information. Don’t forget [**your email**](https://blog.mailfence.com/best-gsuite-alternative/)**:** an [email secured](https://blog.mailfence.com/secure-email-and-end-to-end-encryption/) by [end-to-end encryption](https://blog.mailfence.com/end-to-end-encryption-and-digital-signatures/) ensures that only the recipients you have validated will be able to read the messages your collaborators will send;
* Enable [**Two-factor authentication (2FA)**](https://blog.mailfence.com/harden-mailfence-account/) every time a site or an application offers it.
* Make sure that you regularly **back up**your data on different media, one of which will be kept outside your company. If you can, also implement a **disaster recovery plan**. If your data is compromised, it will be easier for you to maintain your activities, and to avoid financial losses.

**Baiting**:

People like winning prizes. Doesn’t matter if they actually signed up for the game or not. Except that your privacy and security is worth much more than that.

“Congratulations! You won a prize!”

If you ever saw a message like this, there is a 101% chance that it was a baiting attack.

Baiting is like the real-world ‘**Trojan Horse**’in that it relies on the curiosity or greed of the victim. This is different from, say a [quid pro quo attack](https://blog.mailfence.com/quid-pro-quo-attacks/) where the victim might feel obliged to “return the favor”.

It’s in many ways similar to [phishing](https://blog.mailfence.com/what-is-phishing/) attacks. However, what distinguishes them from other types of [social engineering](https://blog.mailfence.com/what-is-social-engineering/) is the promise of an item or good that hackers use to entice victims. For instance, the attacker may offer users free music or movie downloads if they surrender their login credentials to a certain site.

Let’s take an example – with the end goal of infiltrating a company’s network.

Social engineers want to introduce malware into network-connected computers and spread malicious code.

One way they can do this is by promising a reward (“bait”).

For instance, employees can receive infected flash drives as a reward for participating in a survey.

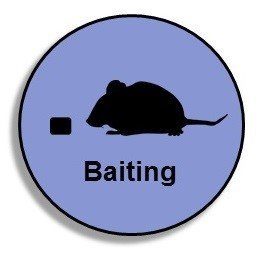
Or, the bad actors can leave infected USB drives in a basket of gifts placed in the company lobby for employees to simply grab on their way back to their work area.

Another possibility is the strategic placement of tainted devices for targeted employees to take. When marked with intriguing labels like “Confidential” or “Salary Info,” the devices may be too **tempting**for some workers. These employees may just take the bait and insert the infected device into their company computers – and Voila!

**What’s the difference between baiting and other social engineering techniques?**

The specificity of baiting is to tempt a victim to take the bait, hence the name. The tempting content could be the **promise**of a gift, or the possibility to get some reward. Therefore, the hacker’s job is to create a **trap**for its victim.

Besides this small subtlety, it’s quite similar to other social engineering techniques, such as [phishing](https://blog.mailfence.com/what-is-phishing/), [pretexting](https://blog.mailfence.com/pretexting/), or [smishing](https://blog.mailfence.com/social-engineering-smishing/).

[](https://blog.mailfence.com/wp-content/uploads/2015/11/a.jpg)

**How to secure your system against baiting?**

The strongest defense against baiting and any other [social engineering](https://blog.mailfence.com/what-is-social-engineering/) scheme is **educating**yourself and your team. Each of us should aim to have a strong security culture within our surroundings – office, home, etc.

In addition, every individual must consider ‘company security’ as an essential part of their individual responsibilities. Specifically for baiting, every individual should do open discussions with his family, friends, and colleagues – and warn them about the dangers of social engineering.

**Educating yourself and others – is by far the most effective defense you can do against all faces of ‘Social Engineering’.**

**Pretexting**:

The best lies revolve around a good pretext and hackers know this well enough. That’s why they’ll try to use all kinds of fabricated scenarios to trick you into giving them your data.

Pretexting attack is a specific kind of [social engineering](https://blog.mailfence.com/email-security-and-privacy-course/) focused on creating a good pretext, or a fabricated scenario, that scammers can use to trick their victim into giving up on their own personal information.

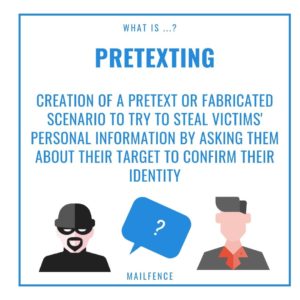
Let’s have a look at some pretexting examples and how to prevent this kind of social engineering.

Pretexting is based on trust. Pretexters can impersonate co-workers, police officers, bankers, tax authorities, clergy, insurance investigators, etc. Simply put anyone who has **authority or a right-to-know by the targeted victim**. These attacks commonly take the form of a scammer pretending to need certain information from their target in order to confirm their identity. The pretexter must simply prepare answers to questions the victim might ask. Sometimes, an authoritative voice, an earnest tone, and an ability to think on one’s feet are all that is needed to create a *pretextual scenario*.

Attackers pretend to have some authority over you and then **ask for both s*ensitive* and *non-sensitive* information**. Back in 2020, a group of scammers posed as representatives from modeling agencies and escort services. They invented fake background stories and interview questions to make women and teenage girls, send them nude pictures of themselves. Later, they sold those pictures to pornographic businesses for large amounts of money.

As a pretexting attack is based on trust, attackers trick their victims into giving up on their own personal information.

**One of the most critical aspects of social engineering is trust**. If you cannot build trust you will most likely fail. A solid pretext is an essential part of building trust. If your alias, story, or identity has holes or lacks credibility or even the perception of credibility the target will most likely catch on. Similar to inserting the proper key in a lock, the right pretext provides the proper cues to those around you and can disarm their suspicions or doubts and open up the doors, so to speak.



**Pretexting examples**

* **Example #1 Internet service provider**  
    
  A person is posing as an employee of your internet provider. They could easily trick you by saying that they came for a maintenance check. First, if you are like the average Joe you don’t know much about network maintenance only that it is required so you can keep watching Netflix. Hence you are going to fall for it and let them “work”. What you can do in this scenario is to ask questions and say that nobody informed you that such a visit would occur. Moreover, you can take this a step further and ask what internet plan you are subscribed to or more advanced questions that only a real employee would know. Check their sources and directly call your internet provider.
* **Example #2 Gift card eligibility**  
    
  You get an email with the subject GOOD NEWS!! You open it and you see that you are eligible for a free gift card. Great right? Who doesn’t like free stuff, especially gift cards? You see a link inside that says fill in your details so you can have it delivered to you. Alternatively, a hacker may first check victim’s availability, to determine if his chosen victim is useful to him and to establish a rapport.  
  It requires first/last name, address, etc. However, ask yourself if someone says you are eligible for a gift card wouldn’t he/she already know your details? On what grounds are you eligible, what did you do for it? Did you compete somewhere? See, this is the part where you should sense that it is likely a scam.  
  Pretexting is not limited to these examples only, scammers will always come up with a new pretexting technique. Your best response would be to arm yourself with knowledge and be aware that such scams will always exist and will take many forms.

Follow this [link](http://www.social-engineer.org/newsletter/social-engineer-newsletter-vol-05-issue-69/#sthash.t7X7pvnD.dpuf) to learn more about it.

**How to prevent Pretexting?**

Scammers exploit human weaknesses to steal your personal information. We do what we can to protect users from this kind of threat e.g. check our [DMARC enforcement strategy](https://blog.mailfence.com/mailfence-dmarc-enforcement-strategy/), but this is not enough. To help you to educate yourself against all kinds of social engineering, we suggest you follow our [email security and privacy awareness course](https://blog.mailfence.com/email-security-and-privacy-course/). We strongly advise you keep yourself informed against social engineering, especially since it’s one of the most common threats to online privacy and digital security.

If you receive an email from someone saying that a maintenance worker will be swinging by, contact the sender’s company, not the sender. Give them a ring and verify that they are sending someone. If you are home when they arrive, ask to speak to their supervisor, don’t take their word for it. Ask for the company’s corporate number and their supervisor’s name, so that you can call from your own personal phone. It may seem rude, but if they are a social engineer, your best defense is to punch holes in their story.

The same applies to websites advertising events and expos. Call the event centre and ask about the event;**go straight to the source**. Beware of any website that only accepts cash or PayPal.

Like any other defence to social engineering, you must be proactive and not reactive.

In any event, your best measure of protection is to hit the source of the pretext. If the social engineer is using pretexting, their weakest point is the fact that **their source doesn’t exist**, it’s all fabricated.

**Common Techniques similar to Pretexting**

All social engineering attacks are pretty similar because they are all based on trust, just like pretexting. However, they all have their specificities. Sometimes, a phishing attack (for example) can be combined with a pretexting attack.

* **Phishing**  
  [Phishing](https://blog.mailfence.com/what-is-phishing/) is another social engineering scam that seeks to steal personal data, such as usernames, passwords, banking details, etc. By using fraudulent websites and false emails, fake phone calls, and whatnot – perpetrators attempt to steal your personal data – most commonly passwords and credit card information. Just like pretexting attacks, they are based on trust. However, phishing attacks tend to trick their victims using fake urgency as well.
* **Smishing**  
  [Smishing](https://blog.mailfence.com/social-engineering-smishing/)is very similar to phishing but this social engineering scam uses SMS texts as opposed to emails and links. Hence the name SMSishing. It tends to be more effective as getting someone’s emails these days is easy. It could be that your email was leaked in a data breach and was sold on the Dark web. However, a phone number is a bit more intimate thus it already creates a sense of connection and trust when you an SMS from your bank or another service.
* **Vishing**  
  [Vishing](https://blog.mailfence.com/vishing/) is another form of phishing but this time it is with voice, hence the name. The social engineer will impersonate the usual services as phishing does. But this time, you will have a person on the other end of the line instead of links and emails. With the right tone, the right questions, and with some patience, this can be really effective against unaware individuals. Especially older people who do not use emails and SMS texts.
* **Whaling**  
  [Whaling](https://blog.mailfence.com/social-engineering-what-is-whaling-attack/) is comparable to phishing, except the victim is specifically targeted as ‘whales’ due to their high rank at a valuable organization. On the contrary, phishing scams get sent massively.

**Phishing**:

In the Q3 2022 there were 1,270,883 phishing attacks. Phishing is getting more and more sophisticated and is the number one threat that email users need to keep an eye on.

Phishing is the most well-known social engineering attack, where a cyberattacker pretends to be a reliable source to make their victims reveal their personal information or download malware.

**According to the**[**National Institute of Standards and Technology (NIST)**](https://www.nist.gov/blogs/cybersecurity-insights/cybersecurity-awareness-month-2022-recognizing-reporting-phishing)**, there are more and more phishing attacks each year, with a staggering rise of 61% since 2021.**

These statistics show the prevalence of phishing attacks and the need to protect yourself against them. Discover how phishing works, how to avoid it, and how to protect yourself and [your company](https://blog.mailfence.com/hackers-target-small-businesses/).

Phishing (pronounced “fishing”) [is a kind of identity theft](https://en.wikipedia.org/wiki/Phishing). In these kinds of [social engineering](https://blog.mailfence.com/what-is-social-engineering/) attacks, hackers will attempt to steal your personal or your company’s data or induce you to download some malware, using a deceptive method to get your trust, usually in an email.

**Various deception tactics**

Deception can be :

* The [**impersonation of a person**](https://blog.mailfence.com/email-spoofing/) or an organization you know, such as your bank or one of your coworkers,
* The **use of URL links** leads you to a fake site that mimics a genuine one you trust. This staged website will have been set up to get user’s credentials.
* Some seemingly useful **files** you’ll be invited to **download**, containing a Trojan horse hiding malicious software (malware).

If it’s the latter, the hidden malware can be :

* Spyware designed to collect data and [**spy on you**](https://blog.mailfence.com/why-companies-should-protect-data-from-spying/),
* **Malware**designed to create a vulnerability, such as creating a backdoor in your IT system or converting your device into a [zombie device](https://blog.mailfence.com/secure-email-practices/),
* More frequently these days, [**ransomware**](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/), malicious software designed to freeze the victim’s device. To unlock it, you’ll have to pay a ransom.

**Many forms of phishing attacks**

There are several types of phishing attacks, depending on the tactic adopted by the hacker to get in touch with his victim :

* Classical phishing : The “phishermen” send**massive emails** to random people. These messages are all identical and they contain a link pointing towards a spoofed website to induce the reader to leave his credentials. Or they invite the addressee to download an attached file infected by malware.
* [**Spear Phishing**](https://blog.mailfence.com/distinguish-spear-phishing-from-phishing/): A phishing attack that targets **organizations and specific individuals** instead of sending bulk emails
* [**Smishing**](https://blog.mailfence.com/social-engineering-smishing/): Phishing attack that, instead of emails, uses **SMS** text. Hence the combination of words SMS+phishing
* [**Vishing**](https://blog.mailfence.com/vishing/): This attack involves the perpetrator **voice** (through a **phone call**) to trick you into completing an action.
* [**Whaling**](https://blog.mailfence.com/social-engineering-what-is-whaling-attack/): An attack that targets “whales” such as **senior & executive members of an organization**. They will usually be induced to execute an action like the transfer of a large amount of money, leading to tremendous rewarding for the attacker.

**How to recognize a phishing message?**

Apart from ensuring you install an anti-spam filter and security software, the best way to combat phishing scams is to identify them.

Spelling mistakes and bad grammar in an email used to be a good telltale of a phishing attack. But nowadays, phishing attacks are more and more sophisticated, and phishing emails are often perfectly written.

**You’ll have thus to focus on other details revealing an attempt to deceive you:**

* **Links in email.** Take the habit of hovering over any hyperlinks sent in an email or SMS to check that they match the site page it’s meant to lead you to as typed in the message. Mismatched URLs **(or misleading domain names)** can also lead you to .exe files embedding malware.
* Links included in an email inviting you to connect to a website. Be especially cautious with any “clearance” or “outlet” website seemingly linked to a legitimate renowned retail portal, for instance. It could be a lookalike website created to steal your ID or some money.
* **Threats –**Have you ever received a threat that your account would be closed if you didn’t respond to an email message? Cybercriminals often use threats. They will send you a fake alert telling you your security has been compromised, a service is about to be terminated due to your inaction, or your banking account is overdraft.
* **Messages**[**spoofing**](https://blog.mailfence.com/email-spoofing/)**popular websites or companies.**In case you receive a message from a trusted organization, a coworker, or a friend requesting you to do something, pay attention to:
  + *Any request**for personal information;*
  + *An offer too good to be true, or some money you should receive or send;*
  + *Any action you didn’t initiate.*

Anything which doesn’t look right should arouse your suspicion. Even emails seemingly coming from specific types of organizations, such as **charities or government agencies**, can be dangerous. Attackers often take advantage of **current events and certain periods of the year**, such as:

* natural disasters (e.g., earthquakes, hurricanes, etc.);
* epidemics and health scares (e.g., [Covid-19](https://blog.mailfence.com/cyber-threats-why-pandemic-responsible/));
* economic concerns (e.g., inflation);
* political elections or events (e.g., the [war in Ukraine](https://blog.mailfence.com/information-warfare/));
* retail good deals;
* holidays;
* …



**How to protect yourself and your company against phishing**

1. Be wary of emails asking for **confidential information** – especially information of a financial nature. Legitimate organizations will never request such information via email, phone calls, or other means. Instead, always pay attention to the sender’s email address. It may imitate a legitimate business with only a few characters altered or omitted.
2. Never open a **suspicious attachment**, as it is a standard delivery mechanism for [malware](https://blog.mailfence.com/viruses-spywares-malware-botnets-protect/). Phishermen like to use **scare tactics** and may threaten to disable an account or delay services until you update certain information. Be sure to contact the merchant directly to confirm the authenticity of their request.
3. Watch out for **generic-looking requests** for information. Fraudulent emails are often not personalized, while authentic emails from your bank often reference an account you have with them. Many phishing emails begin with “Dear Sir/Madam” or other generic greetings/signatures, and some come from a bank with which you don’t even have an account.
4. Don’t get pressured into providing sensitive information, and never submit them via **embedded forms** within email messages – a very common phishing practice and widely pushed onto your junk/spam folders on a daily basis.
5. Never use links in an email to connect to a website, as they could be **spoofed hyperlinks**. The links not matching the text that appears when hovering over them should raise a red flag. It also includes the use of UR-shortening services. Instead, open a new browser window and **type the URL directly** into the address bar (or check where that short link leads to, e.g. see links below). Often a phishing website will look identical to the original, e.g., [https://wwwpaypal.com/](https://www.paypal.com/) is different from https://www.paypal.com/. Similarly, https://www.paypaI.com/ (with a capital letter “i” instead of a lowercase “L”) is different from https://www.paypal.com/ – look at the address bar to make sure that this is the case (and the connection is secure – such as [https://](https://blog.mailfence.com/what-is-phishing/)).

**Even more tips to protect yourself**

1. Make sure you **maintain an adequate environment** to combat phishing. Use anti-viruses and trusted browsers. Keep all your software up-to-date. Use encrypted servicesto communicate and further safeguard your privacy.
2. **Use Password managers** that auto-fill passwords to keep track of which sites those passwords belong to. If the password manager refuses to auto-fill a password, you should hesitate and double-check the site you’re on. Read this blog post to avoid [bad password habits](https://blog.mailfence.com/bad-password-habits/).
3. **Always be suspicious** – Phishing emails try to freak you out with **warnings**, then offer you an **easy fix** if you just “*click here*!” (or “You’ve won a prize! *Click here* to claim it!”) When in doubt, don’t click. Instead, open your browser, go to the company’s website, and then sign in as usual to see if there are any signs of strange activity. If you’re concerned, change your password.
4. Always use [**2FA (two-factor authentication)**](https://blog.mailfence.com/harden-mailfence-account/) when a service provides it.
5. You can **check-test a particular link before opening it** on where it leads to: [Where Goes](http://wheregoes.com/), [Redirect Detective](http://redirectdetective.com/), [Internet Officer Redirect Check](http://www.internetofficer.com/seo-tool/redirect-check/), [Redirect Check](http://redirectcheck.com/), [URL2PNG](https://www.url2png.com/), [Browser Shots](http://browsershots.org/), [Shrink The Web](https://www.shrinktheweb.com/), [Browserling.](https://www.browserling.com/)
6. Last but not least, **learn about new trends in phishing**. You can start by reading our [**Email security and privacy awareness course**](https://blog.mailfence.com/email-security-and-privacy-course/). It is simple and accessible for all, yet informative.

**What should you do if you’re a victim of a phishing attack?**

If you have fallen for a phishing attack, check out our blog post on [hacked emails](https://blog.mailfence.com/hacked-email/).

You can also report the phishing attempts at:

* [Google](https://www.google.com/safebrowsing/report_badware/) – report phishing or badware
* [US-Cert.gov](https://www.us-cert.gov/report) – report phishing
* [Consumer.ftc.gov](https://www.cisa.gov/report) – report phishing

In the future, try to always protect your computer by applying these [10 tips.](https://blog.mailfence.com/10-tips-to-protect-your-computer/)

**How Phishing is evolving : 2023 phishing trends**

Nowadays, phishermen often work for large criminal organizations having substantial resources to improve their techniques and multiply their attempts. As a result, attacks are becoming more sophisticated and harder to detect.

**Here are the phishing trends emerging in 2023:**

1/ Cybercriminals use more often **mobile devices** and **personal communication channels** (social media accounts…) to contact their victims. Indeed, **SMS**has become a popular way to get in touch with potential victims.  (see our article dedicated to [**Smishing**](https://blog.mailfence.com/social-engineering-smishing/))

2/ **Brand spoofing** is getting more sophisticated and harder to detect.

3/ [**Spear Phishing**](https://blog.mailfence.com/distinguish-spear-phishing-from-phishing/)**campaigns** require a lot of preparation. For this reason, hackers used to mainly target big organizations, more apt for providing big rewards (this is called “big game hunting”). But nowadays, due to the optimization of phishing techniques, [**smaller companies are targeted as well**](https://blog.mailfence.com/hackers-target-small-businesses/).

4/ Hackers target [**cloud**access](https://blog.mailfence.com/why-companies-should-protect-data-from-spying/).

5/ Sometimes, cyber pirates are **willing to pay** to obtain user credentials.

6/ Even aspiring phishermen can use these sophisticated techniques, thanks to **RaaS (**[**Ransomware**](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/)**as a service)**. RaaS provides them with a toolbox full of all services and coding bits necessary to launch a ransomware attack against a fee. These tools include the phishing emails templates often used to initiate a ransomware attack.

7/ A new range of cybercriminals, **Initial access brokers, or IABs**, are now focusing on **getting login or email credentials**. They try to steal them by breaking into the information system of organizations. They can **sell them to other cybercriminals** whenever they manage to get them. These will be able to launch very dangerous phishing campaigns with these credentials, since they are legitimate.

**Spear Phishing:**

If phishing is like casting a wide net and hoping to catch a few small fish, spear phishing is using a harpoon to catch the big fish.

Spear phishing is a specific kind of phishing where the victim is targeted and deceived by using accurate personal information gathered beforehand. For example, the hacker can use your public data obtained from your social media accounts to convince you their message is authentic.

Let’s say you’ve just bought a house and posted the news on Facebook. Thanks to one of your comments on LinkedIn, the hacker discovers your banker’s name and agency. From there, he just needs to create a seemingly trustworthy email address using those informations and here it is ! He can then request you to transfer some money to a specific account pretending you must do it in regard of your mortgage. If you are not careful enough, this is how you’ll get scammed.

Sometimes, the authors of this kind of scam can be sponsored by a government. They can also be hacktivists, or cybercriminals looking for sensitive information to sell to governments or competitors.

**What’s the difference between phishing and spear phishing?**

As you could expect given its name, spear phishing is actually a kind of [phishing](https://blog.mailfence.com/what-is-phishing/). “Phishing” encompasses all kinds of cyber attacks aiming to collect sensitive informations (credit card number, passwords, social security number…) through deceiving, theft of identity or impersonification.

**What does a phishing attack look like?**

Phishing attacks are typically launched on a broad scale. They target a vast number of potential victims and are not tailored to them. In most of the cases, all these people are hit at the same time with a spoof email pretending to be sent by an authentic organization.

You’ve likely already been exposed to this kind of scam. We all have received one of these emails allegedly sent by a person resquesting help to move a huge amount of money (typically many dozens of millions of dollars) blocked in a Nigerian bank and offering a significant percentage of this fortune in exchange of our collaboration. Very often, it implies sharing our personal or banking information… Most of the times, these scams originate from Nigeria, which explains why they are called Nigerian Letters or “419” Frauds (419 being the section of the Nigerian criminal code prohibiting this crime).

The perpetrators of these phishing attacks don’t make a lot of efforts to make their message credible. Frequently, their email is somehow gross (spelling mistakes, language errors, cultural hiatus) and the scam is blatant. They simply bet that among the number of people who will receive it, someone will be naive enough to click on the link provided, or send the personal information requested.

**What’s the difference with a spear phishing attack?**

The main difference between phishing and spear-phishing is that in the latter, the hackers target a specific victim, and not a mass of people at the same time.

In a large proportion of such attacks, the victims are executives or employees who hold positions that give them access to certain hardware, software or privileges in the organisation where they work. But they may also be people who have published some exploitable information for scammers (as in our example of the purchase of a house).

Before contacting them, the hackers will have researched them to learn as much as possible about the organisation they work for, the position they hold, how they are called (e.g. use of nicknames), the name of their manager or CEO, the name of a bank where their organisation has an account, etc.

This information is then used to craft a message simulating a genuine email from that organisation, or from another entity with which it is in contact. The scammers will make sure to render it as credible as possible. They will add details that will reinforce the illusion (very similar email addresses, names of real officials, copy of logo, copy of mentions usually included in the emails of this organisation) so that the message seems legitimate to win the trust of its recipient.

They can include an URL to invite the recipient to visit a fake website he may have previously created to collect the sensitive information requested (passwords, social security number, bank account or credit card numbers, etc.). In some cases, they will have taken care to generate traffic to this spoof website to validate the domain name and fool the organisation anti-virus software.

Other times, they may pretend to be a friend, claiming to be in distress and needing a sum of money, or asking for access to specific pictures posted on social networks.

A third form of spear phishing uses an attachment simulating an invoice, or a document of some kind (pdf, Word or Excel file) secretly containing a malicious software, a macro or a piece of code (e.g. a [keylogger](https://blog.mailfence.com/protect-yourself-from-a-keylogger/)). It could also be a [ransomware](https://blog.mailfence.com/top-5-ways-protect-your-device-from-ransomware/), a software that can block the organisation’s computer system, forcing it to pay a ransom to unlock it.

The hackers will frequently explain that their request for sensitive information is urgent. They will tell the victims they need to change a password which is about to expire, or to take notice of changes in a delivery described in an attached document, for example.

They may also impersonate a senior member of the organisation (typically the CEO, or a manager involved in payment transactions, for example) asking for an urgent transfer to a new supplier. Sometimes, this urgency will be combined with the need to maintain strict confidentiality or to breach particular procedures, such as obtaining a manager’s approval.

Finally, they may also play on emotions and try to use empathy to get their victim to obey.

All these stratagems aim at obtaining a quick move from the target, to avoid him/her thinking too much…

When they succeed in their goal, the scammers will impersonate their victims thanks to the personal data to carry out specific operations (money transfer, theft of personal data, theft of intellectual property, unwanted publication of heinous messages on their behalf, etc.). In other cases, they will get their targets to click on a link to trigger the download of a malicious software without their knowledge. Or they’ll get a money transfer or a specific action from their victim.

**Who can be targeted?**

Any employee of an organization can be targeted in a spear-phishing attack. However, some of these scams target more specifically high-level executives. They are called “[whaling attacks](https://blog.mailfence.com/social-engineering-what-is-whaling-attack/)“. Most of them impersonate the CEO or another senior member within the organisation to impose an unquestionable order on the victim.

Remarkably, studies suggest executives are more likely to be targeted, but also more prone to be fooled than other staff members. That’s because they are often very busy and lack of the time needed to dedicate a critical attention to their emails. Sometimes, they also underestimate the threat.

On the other side, it is more rewarding for a hacker to pick them, because of their higher access and authority.

It’s also worth mentioning that these cyber attacks are also frequently launched against employees or executives working in processes involving payments, such as payroll or invoicing.

Finally, note that even individuals can fall victim to this form of scam: a hacker may pose as one of your friends and invite you to click on a nice website or video… hiding a ransomware that could lock your smartphone.

**How to detect this kind of fraud?**

Most of the time, spear phishing emails are very well imitated, which is why it’s very difficult to detect the malicious sheme. Even the tools used to detect preventively this form of scam emails within the organisations can fail to identify spear phishing attacks messages.

This is also the reason why they have become commonplace (it’s estimated that they now account for 91% of all cyber attacks), and why they do so much damage.

**Some advice to help you spot a spear-phishing email**

1. Always double check every piece of information, especially the sender’s details. You may only see the sender’s name but pay attention to the email address as well. It is very unlikely that your banker will send you an email from a “nameofthebanker.nameofthebank@gmail.com” kind of address. Check cautiously the email address provided, even if it seems to come from a trusted organisation. Look for a digit 0 typed in place of an “o”, or for a Russian “ш” spoofing a “w”.
2. Does any detail seem different from usual? Watch out for differences in format. Is the signature different, even slightly? The email is full of spelling mistakes, which is never the case with that specific person ? The way it’s addressing to you is not familiar? All those details are red flags inviting you to be suspicious. Some specific characteristics may not be known by hackers and that’s where you can spot spear phishing.
3. Just like you double check the email address, check any link sent to you. The actual URL is not the same than the link you are asked to click on? It might be something to worry about.
4. Also, pay attention to the wording and the jargon. An unusual mention or expression never heard within your organisation should make you suspicious. Check as well the polite phrases and greetings at the end of the message. Is it usually “Thanks”, or “Best regards”, or something else?
5. Finally, if a click on an attached file triggers the opening of a window indicating that it contains a macro, beware!
6. When in doubt, never hesitate to confirm the content of an email over the phone. A quick call might save you a lot of trouble! *Better safe than sorry.*

**How to prevent spear phishing?**

Hackers can use several tricks to obtain information about their victims. For example, they can use out-of-the-office messages to find out what an organisation’s staff members emails look like. Others will use social media and other publicly available sources to gather information.

**Some advice to help you prevent these attacks**

Beside being careful, you have other options to prevent spear phishing. Hackers might be subtle but being scammed is not a fatality and you can actually protect yourself and your personal data by taking the following steps :

1. Keep in mind that any piece of information (name, picture, …) posted on social media can be used maliciously. When possible, make your accounts private and avoid publishing too much information about your responsabilities, suppliers, clients, processes or operational aspects of your business in your LinkedIn profiles.
2. Avoid publishing too much information about your staff in your website as well. Don’t provide their email, use a form instead to invite visitors requesting for informations.
3. Pay attention to the job advertisements published by your organisation to fill positions in the IT department. Make sure they are never too specific when mentioning details about the software and cybersecurity systems used by your organisation.
4. Look out for these information on Internet too, and suppress them when possible.
5. Always use a hosted email security system and an antispam protection to stop any harmful email.
6. In any case, never send sensitive information like credentials and passwords to anyone. When some attachments are sent to you, scan them with your anti-virus before opening them.
7. Keep all your software constantly updated to avoid any abuse of a security breach.
8. Knowledge and awareness are keys. Keep yourself informed about the [latest phishing trends](https://blog.mailfence.com/email-security-and-privacy-course/).
9. Organisations need to train their staff and organise spear phishing attacks simulations. This way they can develop awareness of this threat and identify which employees are more vulnerable to these kinds of scam.
10. Train your staff to report any suspect email to the IT department, and to avoid clicking on any URL in emails. They should instead connect directly to the genuine website.
11. Beware of unusual and unexpected emails, especially if they claim to be urgent.
12. If your organisation has good skills in its IT department, it may be worth asking them to mark all external emails so that they are easily distinguished from internal emails.
13. Establish strict rules concerning the use of passwords. Forbid your staff to reuse a password, or to use passwords that are too easy to crack.
14. Establish payment processes involving many executive approvals.
15. Avoid any “BYOD” policy and the use of external softwares, platforms or applications not expressly allowed by your IT department.
16. Prevention matters as well, especially for more fragile possible targets like elder or younger users. If someone around you can be an easy target, warn them about spear phishing. If you can, try to keep an eye on their email boxes.
17. Inform your staff, your friends and family members about the risks incurred when sharing personal data on social media.
18. Some tools have been specifically created in order to prevent phishing. Here is a selection you can use in order to control any URL before clicking on it : [Where Goes](http://wheregoes.com/), [Redirect Detective](https://redirectdetective.com/) and [Redirect Check](http://redirectcheck.com/).

**Vishing**:

Not every type of phishing uses email. In vishing, for instance, the scammer uses the phone to trick people into giving their personal information. Unfortunately, this scam is most effective with elderly folk, so if you have someone like that at home help them understand that the “nice man” on the other end is only after their money.

**Vishing is a combination of “voice” and “phishing”. It refers to**[**phishing**](https://blog.mailfence.com/what-is-phishing/)**scams done over the phone. Individuals are tricked into revealing critical financial or personal information during seemingly trustworthy phone calls.**

Vishing is a specific form of [Social Engineering](https://blog.mailfence.com/what-is-social-engineering/), more especially a **phishing** attack made over the **phone**. Like with phishing, the victim is **urged** to share some confidential information because of a fake excuse created by the hacker.

Skilled scammers/hackers have everything in place to sound legitimate:

* **Right information:** they already have your name, address, phone number, and bank details. In fact, all the information you would expect a genuine caller to have.
* **Urgency:** You are made to believe your money is in danger and that you have to act quickly. Fear often leads people to act without thinking.
* **Phone skills:** The phone number appears as if it’s coming from somewhere else (i.e. [spoofing](https://en.wikipedia.org/wiki/Caller_ID_spoofing)). So, you pick up the phone already believing the caller as the number seems convincing.
* **Business atmosphere:**  You hear a lot of background noise, so it sounds like a call center rather than a guy in a basement. The scammers either do have a call center or are playing sound effects. Everything is done to make it sound legitimate.

Consequently, if the victim falls for the scam and provides personal information, they mostly end up becoming a victim of identity theft.

**Some vishing examples**

**Vishing scenario #1**

You come home from work and check your voice mail to see if anybody has called. You play your voicemail and hear the following message:

*“Hello, this is Eva from ABC Telecommunications Company. I am calling you to confirm the closing of your account. Both internet and landline connectivity to your address will be terminated tomorrow morning, May 6, at 8:00 am. Our records indicate that you have an outstanding balance. Please call our customer support at 00-… to settle the final bill payment.”*

This is done to create **urgency** and push you to grab your phone and call the given number. Obviously you don’t want to lose your internet and landline connectivity and want to fix this before anything is cut down. You call the number right away and the ABC Telecommunications Company comes up, giving you an automated way to avoid the closure of your account. You are **asked** to put in your social security or National ID number and the credit card number on your account to **verify** that you are indeed the claimed owner of your account. After you enter both numbers, the line goes dead.

**Vishing scenario #2**

You’re watching TV in your living room at 8:00 pm, and the phone rings. You check your caller ID and it is your bank. You pick up the phone.

*“Hello, this is XYZ bank. In the past hour there have been three unsuccessful attempts to access your account. ABC bank has locked your account to secure it and protect your private information. We are committed to making sure that your online transactions are secure. Please call our Security department at 1-800-Blah-Blah-Blah.”*

You know that you have not made “three unsuccessful attempts to access your account in the past hour”; instead you have been sitting in your living room watching TV. In this case, the purpose here is again to create **panic** and push you to call the given number.

Therefore, you call the number and **give the information asked**to authenticate your identity, such as your bank account number, PIN code and National ID number.

Then, the line dies or – even worse – you are transferred to the real XYZ bank, talk to an agent, and find out that you are a victim of a vishing attack.

**How and why is it so easy?**

Vishing attacks are hard to trace because they ‘mostly’ use [**VoIP**](https://en.wikipedia.org/wiki/Voice_over_IP) (Voice over Internet Protocol). Consequently this means they start and end a call on a computer that can be located anywhere in the world.

And how does your telecommunications company or bank come up on your caller ID when it is actually a number from an attacker? They “[**spoof**](http://www.calleridspoofing.info/)” it.  There are services out there, like Spoofcard, Burner (free mobile app), … that allow you to “spoof” your number so that whoever you’re calling doesn’t know that it’s you.  You can display **any number**you want. As a result, this allows vishing attacks to **look perfectly legitimate**on a person’s Caller ID. Spoofing numbers is sometimes legal (fighting against spam, privacy, etc) and sometimes not (online fraud, ..etc) – depending on regional laws and regulations.

**How to spot a Vishing attack?**

As we just mentioned, recognizing the phone number is therefore not enough to ensure the validity of the phone call.

What are other ways to spot a vishing attack?

* Unless you’ve requested a phone call with a specific organization, always **be cautious** when being contacted by someone saying to be a part of it. Especially if they’re asking for **sensitive information.**
* **Double-check anything.** Scammers will use a fake sense of urgency to make you take bad decisions. Even if your bank is calling you to say there’s an issue with your account, take some **time**to call them back, using the number indicated on their website. You can also contact them by email AND on social media to have **different sources**.

**How to protect yourself from Vishing?**

* **Never call the number given to you or displayed on your Caller ID** (unless it’s a number from a friend, relative, etc.). Take the time to look up the legitimate number (for instance, directly from your bank website) and then call it.
* **Never give out any personal information**– to anyone! As a result, this actually goes for any type of request for personal information. Just FYI: Legitimate companies do not ask for your social security number, national ID numbers, credit card numbers OR PIN’s via phone.
* **Hang up**if you get a suspicious call.  Before calling back the legitime number of the company, do a bit of research on the internet.  However, most probably, other victims will already have published information about it.
* **Pay attention** to what you post online. Just like other social engineering techniques, hackers can use what they find online about you to make their attack more efficient. Avoid posting sensitive information such as your bank name, your exact address, …

If you couldn’t protect yourself from a vishing attack, you can *report* identity theft at: <https://www.identitytheft.gov/>

Contact the organization the scammer pretended to be as soon as possible to let them know somebody might access your personal information. They could provide **specific advice**to protect your account.

**Smishing**:

Did you know that 95% of texts are read in just 3 minutes after sending? And the average respond is 90 seconds! People often don’t even read or check the message before responding.

**Smishing is a social engineering attack using phishing techniques, but sent by text message instead of email. The name is a combination of SMS and phishing.**

Smishing (a portmanteau word made of the expressions SMS and [phishing](https://blog.mailfence.com/what-is-phishing/)) is another [social engineering](https://blog.mailfence.com/what-is-social-engineering/) ploy. It’s a phishing technique involving a malicious text message. In other words, it’s a cyber threat aiming to send you a virus or to make you do something harmful to yourself through a text message.

We tend to be more reactive with our phones. We will respond spontaneously to any message. Hackers know this. By using mobile phone text messages (SMS), they look to trick you into taking an immediate action.

Many smishing attacks combine an SMS and a *‘false sense of urgency’* to leverage this trend more effectively. The malicious SMS sent is conveying a sense of emergency to lure victims in taking action even quicker.

People sometimes tend to be more inclined to trust a text message than an email. In fact, we are very aware of the security [risks involved with clicking on links in email](https://blog.mailfence.com/what-is-phishing/), but this is less true when it comes to text messages.

Attackers particularly like smishing since it’s a low cost attack. An internet phone system (VoIP) server, a burner cell phone and a [spoofing](https://en.wikipedia.org/wiki/SMS_spoofing) method: that’s all you need to send a virus through targeted text messages. With applications such as [BurnerApp](https://www.burnerapp.com/) and [SpoofCard](https://www.spoofcard.com/), it is easy and cheap to purchase a spoofed number to text from.

**What are the risks for smishing?**

Like many cyber threats, a smishing attack aims to steal your personal data, bank account details, passwords or access to websites. Sometimes it also seeks to trick you into doing something: transferring money, giving authorization, or access to someone, for example. This can be a mass attack (several people like you will receive the same SMS) or a very targeted attack prepared in advance comparable to [spear phishing](https://blog.mailfence.com/distinguish-spear-phishing-from-phishing/) (you’ll be the only one to receive the text message).

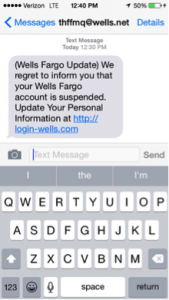
Smishing can lead you to visit a malicious website aimed at stealing your credentials or personal data. Alternatively, you could be led to call a fraudulent phone number. From then, cybercriminals on the phone could also launch a [Quid Pro Quo attack](https://blog.mailfence.com/quid-pro-quo-attacks/) or a [Pretexting attack](https://blog.mailfence.com/pretexting/) against you to get some sensitive information. For this, they would impersonate a manager of your company, a police officer, a security guard to ask you to give them your credentials.

But the most common risk is downloading a virus through the text message sent, or any other kind of malware, such as a Trojan horse. This could turn your phone into a [zombie](https://blog.mailfence.com/secure-email-practices/), allowing hackers to control it. As a zombie device, it could become part of [a botnet](https://blog.mailfence.com/keep-your-private-email-account-secure/), and used to launch a [Distributed Denial-of-Service (DDoS)](https://blog.mailfence.com/ddos-attacks/) attack, or to send some spam, …etc.

**Examples of smishing**

**Scenario #1**

In this example, a malicious text message to “Update information to avoid account suspension.”

Source: http://numbercop.tumblr.com

**Scenario #2**

In this second example, the SMS sent tells you to opt-out from something, or you’ll risk to have some kind of charges to pay.

“Dear user,  
You will be charged 25 Euro per week, under the new Electric supply regulation. If you want to opt-out, please visit www.smished.com (example link)  
Regards,  
Your Electric supply company”

**Scenario #3**

This third example is a kind of [baiting attack](https://blog.mailfence.com/what-is-baiting-in-social-engineering/) : the malicious text message tells the target they can get free vouchers.

“Dear user,  
Aldi is offering a free £65 voucher on your next Aldi visit.  
Please register on www.smished.com (example link) to reserve your voucher in advance”

**How to recognize Smishing?**

Any SMS coming from a phone number that doesn’t look like a phone number, such as ‘0420’ – could be a sign that this text message is actually an email sent to a phone. This could also mean it’s a smishing attack, and that the text sent could contain a virus. In fact, some hackers will use an email-to-text service to send their text message virus or any other kind of malicious SMS to hide their actual phone numbers.

Another smishing method uses number spoofing. The hackers will purchase a spoof copy of an actual phone number to make their text message appear on an existing thread of genuine messages from the bank, store, …etc. In addition, attackers also use [Flash SMS](https://en.wikipedia.org/wiki/SMS#Flash_SMS), to immediately catch the recipients’ attention (e.g. for emergency alerts, traffic alerts – or for receiving one-time pass-codes, …etc).

**How to protect yourself from Smishing?**

* Don’t click on links you get through an SMS on your phone unless you know the person they are coming from. It could be a fake website made up to collect your personal data, banking account password or credentials without arousing your suspicion.
* Be very careful with messages asking you to take immediate action. Don’t feel pressured into responding back ; in most of the cases, legitimate organizations give you the time to react. Make sure first that these messages come from a trusted source. If necessary, confirm their origin by calling the sender directly, after looking up for their phone number on their website. Also, you can generally find your bank’s number on the back of your card.
* Even if you get a text message containing a link from a friend, consider verifying it first with the sender before clicking on the link.
* Be cautious with unusual short phone numbers. They can be issued by email-to-text services, used by hackers to hide their actual phone number.
* Never install any app by clicking on a text message. Always use official app store for installing apps.
* Never give away any personal or financial information by SMS or phone call.
* Don’t reply to text messages coming from people you don’t know.
* Avoid recording any banking information or card number on your phone. Even if your phone falls prey to a virus set up through a smishing attack, the hackers won’t be able to steal them.
* If you’re an organization, [train your staff](https://blog.mailfence.com/email-security-and-privacy-course/) to follow our advice and to recognize all cyber threats and apply cybersecurity rules. They must refrain from sending confidential data via phone or email.
* Learn these [10 tips to protect your computer](https://blog.mailfence.com/10-tips-to-protect-your-computer/) to minimize any impact an attack could have on you or on your business.
* If you’ve been a victim of smishing or know that someone used your name for a smishing attack, you can also report identity theft at: https://www.identitytheft.gov/.

**Scareware**:

You have a virus! Or is it just what the scammers would have you believe?

**Scareware is a**[**social engineering**](https://blog.mailfence.com/what-is-social-engineering/)**technique that aims to scare the victim into believing they have a virus on their device and should buy or download specific software.** **As many social engineering techniques. It’s based on human emotions, as it is used to scare someone and trick them into downloading malware**.

If you ever saw a pop-up on your screen saying something like “Warning! Virus Alert!” or “Warning! 5 Virus Detected!”, that’s scareware in action. The idea of scareware is to convince the user through fear that their device is infected with a virus (or several) and that they should take immediate action and download or purchase the malicious software.

Scareware, which is a combination of the words “scare” and “software” plays on human emotions and reactions.

However, unlike [baiting](https://blog.mailfence.com/what-is-baiting-in-social-engineering/), which promises to reward the user, scareware looks to build anxiety and fear to manipulate the user. Also, unlike [smishing](https://blog.mailfence.com/social-engineering-smishing/), which uses SMS, scareware works across devices and on both desktop and mobile.

**Examples of Scareware**

* In 2009, Mac users began receiving scareware to purchase or download fake antivirus software such as **Mac Security**and **MacDefender.**This scam was later tied to the Russian online payment system **ChronoPay.**
* In 2010, a **Best Western** ad was used to redirect visitors of the **Minneapolis Tribune** website to fraudulent websites, which infected their devices with malicious software.
* A scareware campaign from 2009 to 2016 targeted **OfficeMax**and **Office Depot**customers to convince them to buy a repair service following a fake **PC Health Check**“warned” them that their devices were infected with a virus. Because of this, Office Depot had to pay $35 million to the Federal Trade Commission (FTC) for deliberately tricking its customers.

**How to Spot Scareware?**

Scareware typically comes in the form of a pop-up that is made to look like it comes from a software company, and it has five common red flags:

* It comes from a software company you’ve never heard of.
* Somehow, the software has already scanned your device and detected all these viruses.
* Good luck closing the pop-up window, as the closing button (x) is either well-hidden or hovering the mouse close to it will open a new pop-up over the previous.
* You “have” to act fast! There’s usually a big red button (sometimes flashing, just in case you’ve missed it somehow) that will tell you to “download now!”
* The pop-up headline will always be something like “Warning!” or “Virus Detected!”

**How to Avoid Scareware?**

Knowing how to spot scareware is the first step in avoiding it. Here are some additional tips:

**1. Do Not React Immediately to the Pop-Up**

The attackers are trying to play on your emotions and are using scare tactics to manipulate you into making a hasty decision. They’ll also do in another social engineering attack, called [whaling](https://blog.mailfence.com/social-engineering-what-is-whaling-attack/). Do not react immediately. Instead, take a deep breath and slow down.

**2. Think Rationally**

Read between the lines. There is much more to the “warning” that pops up on your screen than meets the eye.

For instance, have you ever heard of this particular software security before? Know that legitimate companies, like Norton, Kaspersky, and others will never, NEVER do something like this.

Also, how is it possible that they already scanned your device and detected those viruses if you never interacted with them or their software in the first place?

Usually, you have to download the antivirus software on your device and tell it to scan for malicious software. Even then, a virus scan can take anywhere from a few minutes (for a quick scan) up to several hours, sometimes (for a full scan).

**3. Don’t Click on Links that You Don’t Know Where They Lead**

Don’t click on a button or a link just because it says “click me!”. If you are unfamiliar with this company or the URL looks suspicious, it will likely lead you to a malicious website or download infected software on your device.

**4. Don’t Close the Notification, Close the Tab or the Browser instead**

Lots of scareware pop-ups use a fake **Close**or **X**button that clicking on will actually download malware on your device instead of closing it. This is called **Clickjacking.**

To avoid this, close the tab with the pop-up or even the entire browser instead.

**5. Use Firewalls, Pop-Up Blockers and URL Filters**

Use these three to stop pop-ups from appearing on your screen and facilitate this social engineering attack.

**6. Use Only Legitimate Security Software**

Again, legitimate security software companies will never send you pop-ups like these, even more so if you are not their user.

Use trusted antivirus software to regularly scan and remove viruses from your device instead of believing that a random pop-up magically detected a virus (or 50) on it.

Learn more on how to [protect your computer effectively.](https://blog.mailfence.com/10-tips-to-protect-your-computer/)

**How to Remove Scareware?**

If you skipped all of the above and still downloaded the scareware, don’t worry, you can remove it.

First of all, how can you tell if you have scareware on your computer?

* Your device starts to run much slower than normal
* Unwanted pop-ups and ads start appearing on your screen
* You can’t install a legitimate security software

Having a legitimate third-party antivirus tool is crucial to remove scareware from your device. Indeed, it can detect and clean up the infection that the scareware caused in the first place.

Once your device is free of actual viruses and malware (and not the fake ones that the scareware told you about), you can eradicate the offending program from your device.

**On Windows PC:**

1. Open the **Control Panel**.
2. Select **Programs**.
3. Find the scareware application and right-click on it. Common ones include **Mac Defender** and **PC Clean Pro.**Sometimes they’ll even use knock-off names of legitimate tools like **MS Antivirus**(copies the name of **Microsoft Antivirus)**.
4. Select **Uninstall**.

**On Mac:**

1. Go tothe **Finder**window.
2. Open **Applications**.
3. Find the scareware program and either right-click on the icon and select **Move to Bin**or drag and drop the icon to the bin.
4. Right-click on the bin icon and select **Empty Bin**.

**Shoulder Surfing**:

Sometimes, you need to have eyes on the back of your head. Because you can never know who is looking over your shoulder and stealing your information.

**Shoulder surfing is the practice of stealing sensitive information by looking over another person’s shoulder while they are keying that information into the device**.

You’re on a bus, reading the newspaper or something on your screen, when you feel a sensation at the back of your brain. You turn around to see the person behind you quickly retreat. They were looking over your shoulder, or in other words, “shoulder surfing”.

What they were doing was rude, yes, but ultimately not illegal. Now, if you were, say, typing something like a password and they happened to be watching, that’s the first step before**identity theft.**

As a form of [social engineering](https://blog.mailfence.com/what-is-social-engineering/), shoulder surfing happens when a third party looks over the shoulder of another to see the information they are keying into, say an ATM, laptop, smartphone, etc.

**Examples of Shoulder Surfing**

Usually, this happens in crowded places. That’s when it’s easy for someone to stand behind another person and take a peek over their shoulder. However, it can also be done from a distance using binoculars.

Let’s go over some hypothetical shoulder surfing scenarios.

**Scenario 1:**

You are at the airport, and you’re rushing to check in. But before that, you remember that you need to grab some cash. So, you run to the ATM, enter your PIN, grab your $100 and run to the gate.

As you wait for your plane, you get a notification on your phone. You look at it only to see that someone has withdrawn $500 from your card.

**Your mistake:**In your rush, you neglected to spot the person standing just a few feet from the ATM. In addition, you also didn’t take the receipt or make sure that the transaction was complete.

By the way, here are some [tips to protect your devices when travelling](https://blog.mailfence.com/protecting-your-devices/) and to [protect your data when crossing borders](https://blog.mailfence.com/protect-data-crossing-borders/) while we’re at it.

**Scenario 2:**

This time, you are in a cafe. The only spot to sit you could find was at the bar. You take it and open your laptop to pay some bills. People bump into you, but you pay them no mind as you type your login info for the bank account.

Meanwhile, you order a drink from the bar. As you pay for it, you are momentarily distracted from your laptop to give the money to the bartender. Thinking nothing of it, you turn your attention back to the screen while sipping your beverage.

**Your mistake:**Again, you didn’t pay attention to your surroundings, and entered your username and password in plain view. Then you got distracted just enough for someone to see your login information on your screen.

**Scenario 3:**

You’re on the bus, and your spouse is calling you. They need to pay something with your credit card but can’t remember the PIN, so they’re asking you for it.

Over the phone, you go: “3-5-1-6. Did you get that? Okay, bye babe”.

Yes, they did get that, but so did about a dozen or so strangers on the bus with you. If they were paying attention, they now have your PIN.

**Your mistake:**Shoulder surfing isn’t just visually looking over someone’s shoulder to see what keys they are entering. It can also be done by listening in situations like these. By declaring your PIN out loud, you have made it publicly known.

Of course, if anyone else calls you or sends an SMS asking you to reveal some sensitive information over the phone, don’t do it. This is called [vishing](https://blog.mailfence.com/vishing/) and [smishing](https://blog.mailfence.com/social-engineering-smishing/) and both are also types of social engineering.

**How to Prevent Shoulder Surfing?**

So how do you prevent shoulder surfing? Here are some tips:

* First, **always be aware of your surroundings**. Whether you’re in an ATM line, cafe, airport, bus, etc. be sure to look around. Even that small act will often discourage the would-be shoulder surfer and make them leave the spot or at least make them more hesitant to peek over you.
* When using the ATM, always **shield the keypad**as you enter your PIN. Lean over it to cover the view of any potential “onlookers”.
* Again, when using an ATM, make sure to select “Exit” when asked “Would you like to make another transaction?” and take the receipt. Some ATMs don’t require the card to be in the ATM when making an additional transaction, so the shoulder surfer can simply step in behind you and re-enter your PIN to get some cash for themselves.
* If you’re in a public space like a coffee shop, and you need to enter some financial information, do so with **your back turned to the wall.**
* If you need to share sensitive information over the phone, do so away from curious ears. Better yet, send them the info via a message on the phone.
* Don’t leave your laptop unattended. If you need to quickly leave (for the toilet or to another coworker’s desk, for instance), be sure to lock the screen and close the laptop. Of course, if you’re in a public place, you shouldn’t leave your laptop lying around as someone might snatch it while you are away.
* **Use biometric authentication**instead of PINs and passwords. Many devices today allow you to log in and access your data using fingerprint or facial recognition. It is something that the shoulder surfer can’t do anything with. [2FA](https://kb.mailfence.com/kb/setup-2fa/) is also a way to prevent anyone but you from accessing your accounts, even with your password.
* **Use contactless payment.**Again, instead of entering a PIN, use contactless payment apps whenever possible. Remember, the best way to obscure your PIN is not to have to use it at all.
* **Obscure passwords when typing them.**If you need to enter a password to log in to an account, be sure that the password field returns an asterisk field like “\*\*\*\*\*\*\*”.
* **Use a screen protector.**Most folks think of screen protectors as something you put on your phone to avoid the screen being scratched. However, some can also be used to obscure whatever is on your screen and protect your information, so they’re very useful to have.

**Whaling**:

Why catch small fish when you can get a lot more from the big kahuna is the logic behind this social engineering attack that targets the companies leaders and bosses.

**A whaling attack is a social engineering technique involving scam emails imitating senior individual messages to target high-ranking executives. As such, it’s a form of executive phishing, like spear phishing. However, whaling specifically targets one high-profile employee.**

A whaling attack is a form of [phishing attack](https://blog.mailfence.com/what-is-phishing/) usually using fraudulent emails which target executives or managers. The technique is similar, but the fish is bigger. While [phishing](https://blog.mailfence.com/what-is-phishing/)scams get sent massively, a whaling attack targets specific individuals considered as ‘whales’ due to their high rank in a valuable organization (CEO, top-level executives). By impersonating a CEO or a top-level executive, cybercriminals try to trick their victims into doing unfavourable actions. They usually try to get large wire transfers, sensitive information or insert malware with fraudulent links. The latter two mean that this [social engineering](https://blog.mailfence.com/what-is-social-engineering/) technique can have longer-term consequences, because the cybercriminals can launch further attacks with the data retrieved from a whaling attack.

**How to identify whaling attacks ?**

It can be hard to identify a whaling attack. Cybercriminals put a lot of effort into elaborating these scams as the returns can be huge. In the past, they have tricked many highly-educated employees and caused substantial losses for their companies. To avoid this, organisations with sensitive information or a high monetary value should keep their employees informed about social engineering tactics.

**How to recognize whaling scams emails ?**

Whaling emails can display the following characteristics :

* **Personalisation:** The email sent to initiate the whaling attack will most likely include personalised information about the impersonated CEO or senior executive, the victim (a manager or another executive), or the organisation to create a sense of familiarity.
* **Urgency:** Whaling scams emails conveying urgency can get the victim to act before thinking of security practices. Attackers often try to frighten victims using powerful personas (CEO, top level executives). Those persons are difficult to disobey.
* **Language:** Business language and tone are often used to convince the victim that the email has been sent from a high-ranked individual. The attackers often use a scenario in which they ask the victim to do a low-effort action (such as a quick money transfer to a supply partner) based on a fake threat. They may also emphasize confidentiality, so that the victim avoids speaking about the email they have received. No one can thus tell them that this email is a whaling attack.
* **Legitimate signature:** The attackers may use a believable email address, signature, and a link leading to a fraudulent website. We will show you how to recognize these further down the article.
* **Files & Links:**Cybercriminals may use attachments or links to insert malware or to request sensitive information. Even if nothing happens when the targetted manager clicks a link or submits information on its website, it could trigger a hidden malware download.

**Whaling attacks examples**

* From ‘within’ the company

In 2016, a [top finance executive of Mattel got a fraudulent email from someone impersonating the new CEO](https://www.cbsnews.com/news/mattel-vs-chinese-cyberthieves-its-no-game/). This email contained a regular request for a transfer in favour of a new vendor payment to China. After the victim fell into the phishing scam, the company lost $3 million. They managed to get all the money back after an arduous fight.

* From a third party

The following email scam tricked a handful of executives from different industries. The cybercriminal sent a [fake email from the United States District Court](https://www.nytimes.com/2008/04/16/technology/16whale.html) with a subpoena to appear before a grand jury in a civil case. The emails included the executives’ names, companies, and phone numbers, deceiving them that it was official. When they clicked on the link for the subpoena, they got malware.

* With phone calls

The [National Cyber Security Centre](https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it) (NCSC) of the United Kingdom confirms that phone calls from the cybercriminal authors can back the whaling attack itself. A simple trick such as this can make their scam believable. Fortunately, there are ways to prevent falling for one.



**How to protect yourself from a whaling attack ?**

In addition to making them lose money or data, whaling attacks can affect the reputation of the victim and their organisation. Some companies have fired some of their employees because they had fallen for social engineering tactics. For instance, [FACC have given the sack to their CEO](https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF) for this reason. Unfortunately, [according to HP](https://press.hp.com/us/en/press-releases/2020/cyber-attacks-to-become-more-targeted-in-2021.html), these kinds of [cybersecurity attacks increase year after year](https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/) along with their targeted victims.

To avoid being part of the victims of whaling attacks statistics, we recommend following these tips:

**Be aware**

There are different types of whaling attacks and that they can be difficult to spot. When receiving a particular request, remember to:

1. Double-check the sender’s email if it’s sent from a colleague, especially if it’s a high ranking executive in your organization. When the email comes from a third party, search for the authentic email address of this company and compare the two of them.
2. Check if the domain on the link corresponds to the domain name of the company it’s meant to be sent from. If it differs, even slightly, it probably means it’s a fake email trying to impersonate an email from this company. If so, there is probably an associated fraudulent website you must avoid connecting to. Hover over the embedded link with your mouse. You should see the associated domain name appearing at the bottom-right corner of your browser, so you can compare it with the actual domain name of this company.
3. Check the suspicious website’s domain age to see if it matches the trusted one. If the suspicious domain is younger, then you should not trust it.
4. Question the validity of any request for money or sensitive information, even if it’s coming from one of your managers. In case of any doubt, do not hesitate to contact him directly by phone to get his confirmation.

**Know the power of social media**

Anything posted online can work against you. A whaling attack email could be personalised with photos, names, dates, and many other details found on social media. Cyberattackers also commonly use published content published following conferences or company events, meaning that employees should pay extra attention to potential scams after participating in these, since scammers could likely refer to them.

A good practice is to set personal social media accounts to be private. However, it does not fully protect from content published by the company’s public channels (newsletters, social media, website, etc.). The next tip can help with this issue.

**Adopt company-wide data protection policies**

A common understanding of what type of information can be shared publicly prevents cyber attackers from using it. By establishing cybersecurity [best practices](https://blog.mailfence.com/email-security-10-best-practices/) within your company, you can develop a sense of responsibility and accountability among your teams. Therefore, these policies can protect your company against whaling attacks or even spear phishing attacks, and help you avoid substantial losses.

**Some data protection policies that companies take against whaling attacks are:**

* **Flag third party emails:** makes it easier to identify email scams pretending to be sent from colleagues, managers or other senior executives.
* **Verify requests:** when getting particular or urgent requests from a manager’s or high-ranking executive’s email, it is a good idea to confirm who’s the actual sender with them. Talking in person, via a message, or a call can reassure you that it is not a scam.
* **Multi-step verification:** any request for a wire transfer or sensitive information should go through various checks with different people before being operated. For example, having two people sign each high-value money transfer is a simple step that goes a long way. It also lowers the fear factor of being the only accountable employee for such transactions, allowing more clarity needed when making important decisions.

**Anti-social engineering tools and courses**

Scammers will always be a step ahead of the restrictions they face. Using tools and [cybersecurity courses](https://blog.mailfence.com/email-security-and-privacy-course/) can help you identify the patterns of their tricks and prevent whaling attacks as much as possible. For example, a good practice could be for the IT department to send out fake whaling attacks emails to the company teams. By testing their reactions and giving them advice in the feedback of this simulation, the company can train its employees to adopt a safer behaviour.

As for tools, there is anti-phishing software that can recognize fraudulent links and malware downloads. Also, a secure and private email provider, can keep away spam, ads, trackers, hackers and solicitations. Such tools can give users peace of mind from many social engineering tricks.

**What to do if you fell for a whaling attack ?**

If you suffered from whaling or any other social engineering attack and/or your email got hacked, read our blog post on [Steps to take when your email is hacked](https://blog.mailfence.com/hacked-email/). It explains how to control the damage, report it and prevent future hacking attacks.

If you were using a work device or account, communicate with your supervisor and the IT department as soon as possible. They will then be able to alert other employees and ensure that everything stays secure. Also, the sooner you report the incident, the less time the attackers have to worsen the damage. Your organization can set up a complete communication plan involving all affected parties earlier on.