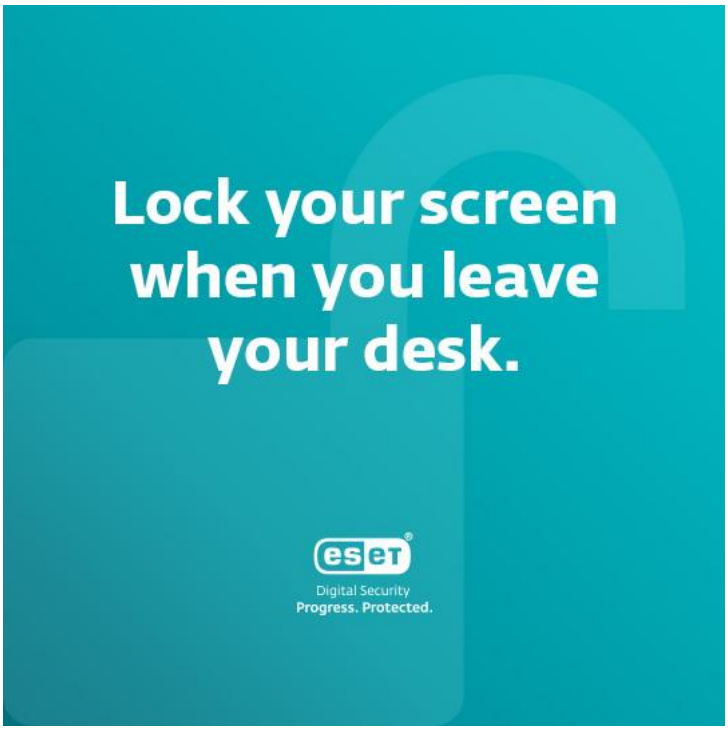



Lock your screen when you leave your desk.

While some passersby might only want to surprise you by sending a seemingly funny email from your account, others might be searching for information they can misuse. Protect your company's sensitive data by always locking your screen when leaving your computer unguarded. Here are the shortcuts you can use to lock your screen immediately.

- Press Control + Command + Q for Macs
- Press Ctrl + Alt + Delete, then Click on LOCK for PCs

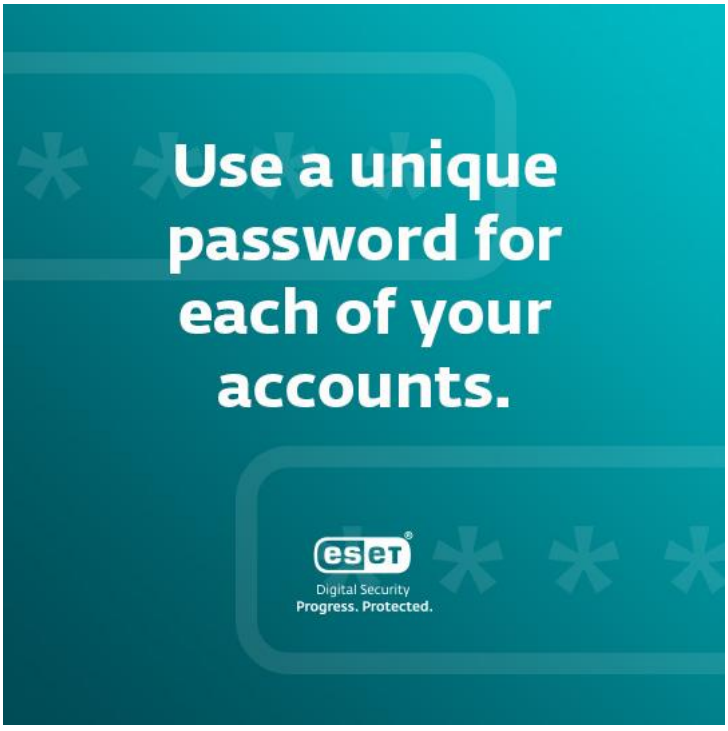
## Change your password into a passphrase.

A good password is easy to remember but difficult to guess. The longer, the better. The simplest way to achieve that is upgrading your password into a passphrase. How can you create a good one?

1. Ideally, a good password or a passphrase should include a combination of uppercase and lowercase letters, numbers, and special characters.
2. Include information only few people know, such as your old childhood nickname, favorite movie, or an inside joke.
3. Avoid information that is easy to find, such as the names of your pets or your birthday.
4. Substitute some words or letters with numbers and symbols. Instead of “someone,” try “s0mE_1.”
5. Add something random. If you choose, for instance, a phrase from a movie or a song lyric, someone has probably done that before, which makes the password easier to crack. Try to add something unrelated that only makes sense to you.

Example:

Change “The greatest month is December.” into “tHeGr8est-M0nthIZ12Decem8er!”




## Use a unique password for each of your accounts.

Maybe you think that it doesn’t matter if someone hacks the password for your IKEA customer account. You may be right – as long as you don’t use the same password for your other accounts, including the work ones. When you re-use the same password for every

account you have, it may be easier for you to remember, but it is certainly not safe. Take some time to go through your accounts and change your login credentials so that you use a different one for each account.


Speak to IT about using a password manager.

If you use secure passphrases or a unique password for each of your accounts, it may be difficult to remember all your credentials. Password managers help with that. When storing your credentials in a password manager, you only need to remember one password while maintaining your security at a high level. Ideally, you can also enable MFA (multifactor authentication), which makes the password manager more secure. Some password managers also offer special functions, such as storing confidential documents! Your IT department can help you pick and install a password manager that is secure and easy to use.


Consult with your IT specialist about installing new apps on company devices.

Want to install a new app on your work device? Always consult your IT team. They should determine whether the application is safe – based on, for instance, how it handles data, how much access it demands, or what happens to its customers when the app goes out of service. Your IT specialist can explain how the app works and how to use it safely in order to protect both your own and the company's digital security.


Think twice before clicking on links in your emails.

Get to know phishing and the tactics cybercriminals use to lure you into their traps. Here are some examples. Remember the basic signs of a phishing email: generic salutation, poor grammar, a mismatched URL, a subject that does not correspond to the body of the message, a sense of urgency, and a demand for quick action. Often, people get tricked by phishing emails because they act under pressure. Take your time to read your emails cautiously and remember that opening the mail itself is usually harmless. The possible danger resides in unknown links and attachments, but also in pictures included in the message, which may enable the attacker to guess your location, device, operational system, and more. The criminal may then use this information to attack you in the future, so disabling automatic picture loading is a good idea. If you spot a phishing attempt, always notify your IT department.


When it comes to strangers in the office, trust but verify.

Whenever you see someone unknown walking around your office premises as if they're lost, ask them whether they need your help. If they seem suspicious to you, don't be afraid to let the security know. As with other things, it is better to be safe than to deal with a data breach due to a malicious intruder. Does this scenario seem unrealistic? Read the story of how Jake Moore, a cybersecurity expert, went undercover and hacked a company because of poor employee awareness.


Mind what you keep on your desk (and in your bin).

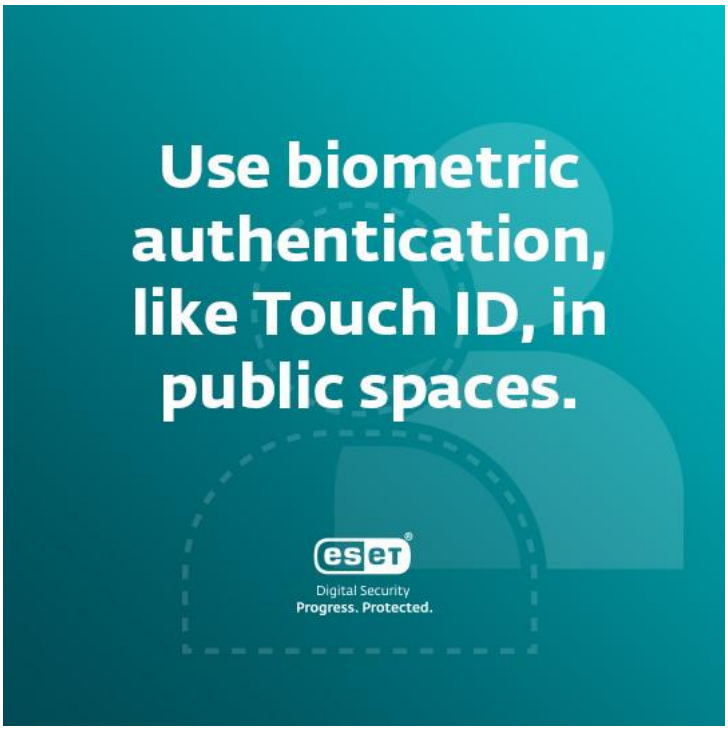
Nowadays, we tend to focus on digital data more than on physical documents. Still, if the latter were to leave the work premises and be seen by a stranger, it may endanger your company. In order to avoid this situation, always shred confidential documents before throwing them away. Additionally, don’t forget to check what’s on your table. Are there any papers no one should read? Or important notes you don't want to share? Better keep them in a lockable cabinet.

Avoid connecting to public Wi-Fi networks.

Places with public Wi-Fi seem attractive – not only to you, but also cybercriminals. This can result in public Wi-Fi systems being infected with malware (via the router), fake public Wi-Fi connections that have been set up by hackers, or the so-called Man-in-the-Middle attacks (MitM), during which cybercriminals position themselves in between you and the connection point and collect your data. If you really need to connect to a public Wi-Fi, always keep your VPN on and do not visit sites that demand you to enter your login credentials, such as internet banking.

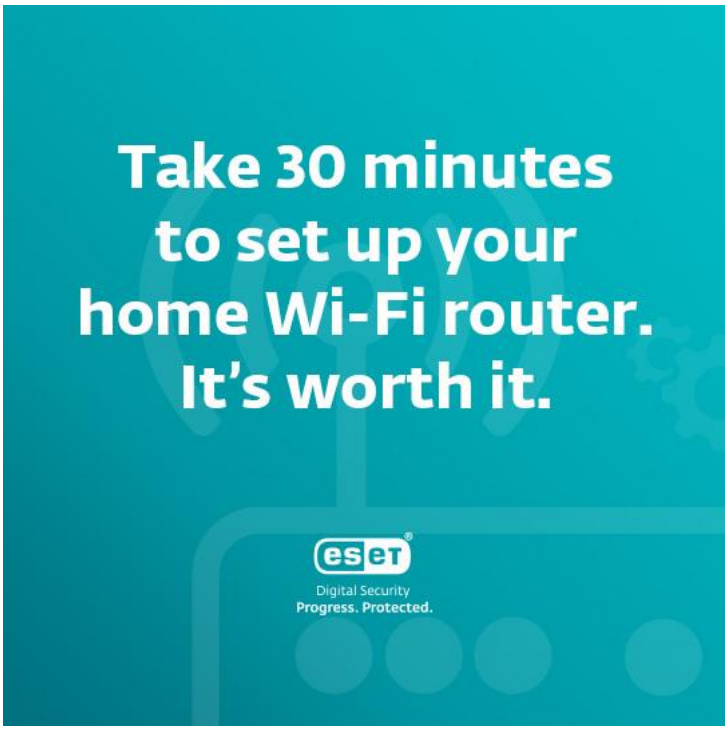

Be careful during video calls and screen sharing.

For many, video calls have become an integral part of their work. But just like when you're dealing with someone in person, there are certain rules to follow to avoid any risk. If you need to share your screen, make sure you are only showing the windows that need to be shown and there are no private documents in the background. The same also applies for your surroundings. If you can, blur your background and always check whether there is anything behind you that isn't safe to share – such as a whiteboard with notes from an internal meeting.



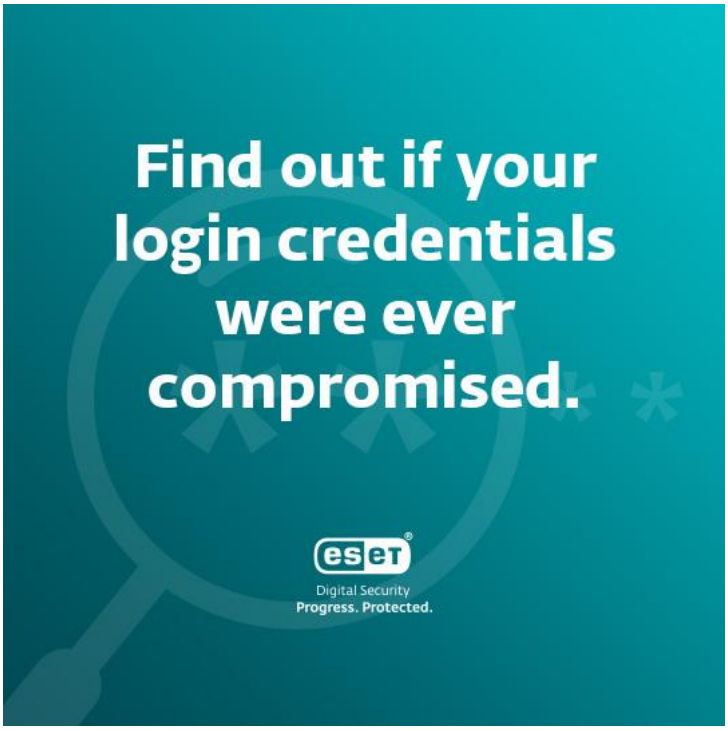

Use biometric authentication, like Touch ID, in public spaces.

Need to log in to your work accounts while on a bus? Or make a work phone call while in a cafe – or even in your own garden? Keep in mind that the people around you may take advantage of that. If anyone sees your login credentials, they can use them to get into your accounts, so when you're in public, use biometric authentication, such as Touch ID. When working remotely, know that anyone outside your company may be able to see what is on your screen, including sensitive documents, so consider getting a screen privacy filter. Also, remember that anyone could be listening to your work phone calls and making use of any of the sensitive information you share. It is always better to only discuss confidential topics when you know you are not being listened to.




Take 30 minutes to set up your home Wi-Fi router. It's worth it.

Working from home has become a standard for many. Substitute your default credentials (including the name of your Wi-Fi and the default password) with a safe password or a passphrase. You should also turn off remote management, keep your firmware updated, and enable network encryption – ideally WPA3. Not sure how to do that? Here are some tips – and if you're still unsure of how to proceed, you can always contact your IT department. Without these preventive measures, it is fairly easy for any outside intruder to get to your data, both work-related and personal.



## Find out if your login credentials were ever compromised.

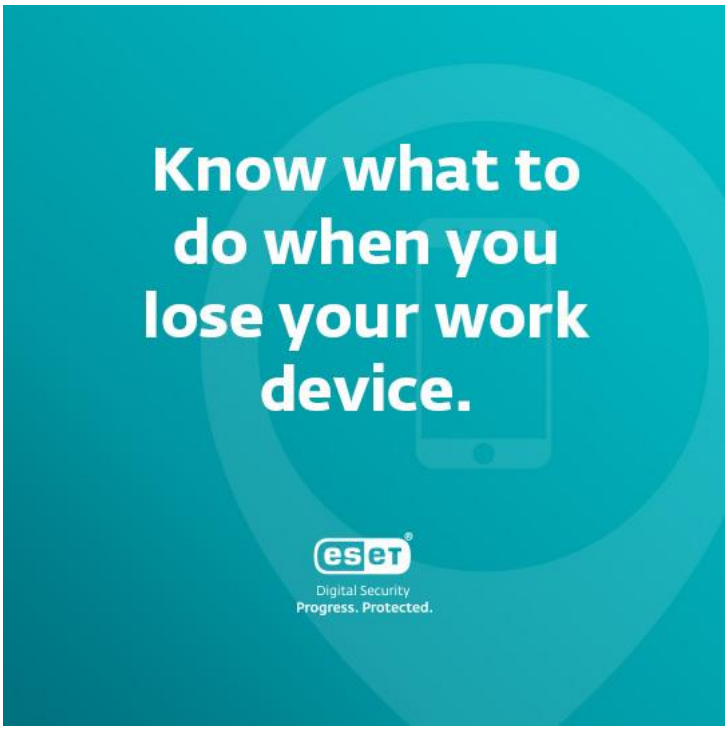
Go to the website Have I Been Pwned, enter your email address, and find out whether your credentials were ever included in a data breach. If the answer is yes, set up a strong password on the compromised accounts – and all others.


## Be careful about what you share on social media.

Want to share a selfie from the office? Or a fun picture of your work desk? By showing others the environment you work in, you may make it easier for an intruder to orientate in the space and make it seem as if they belong there. Additionally, you may unknowingly share some sensitive information about your colleagues, employer, or yourself – for instance, if the picture of your desk contains sensitive documents or sticky notes with credentials. Before sharing anything work-related, make sure it only contains publicly known information.

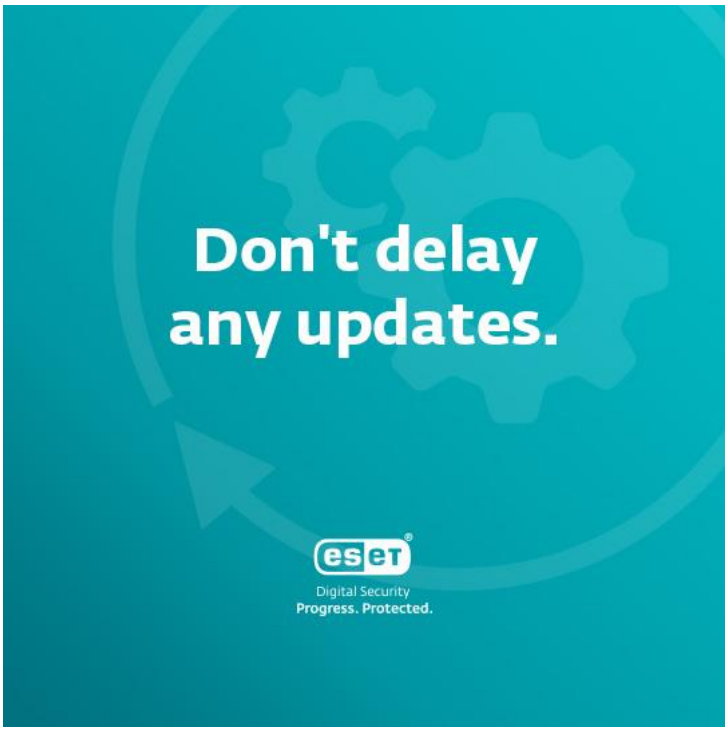

Only use your work device(s) for work purposes.

Sharing is caring, but not when it comes to work devices. While you may be tempted to let your children use your work computer to play games or watch a movie, your device likely contains data that should not be shared with anyone outside your workplace. It only takes a few incautious clicks and the sensitive data on your laptop may be out there for the world to see. Ideally, only use work devices for work-related practices, and don't let anyone else use them.



## Know what to do when you lose your work device.

Losing your work device is unpleasant, but we all know it can happen from time to time. In addition to being careful with your company's equipment (you are responsible for it), you should know what to do when such a situation occurs. Don't hesitate to contact your IT department so that they can solve the issue quickly. And even if you have never lost any work device, it's best to be prepared. Ask your IT department what to do in these situations and get to know the proper procedure.

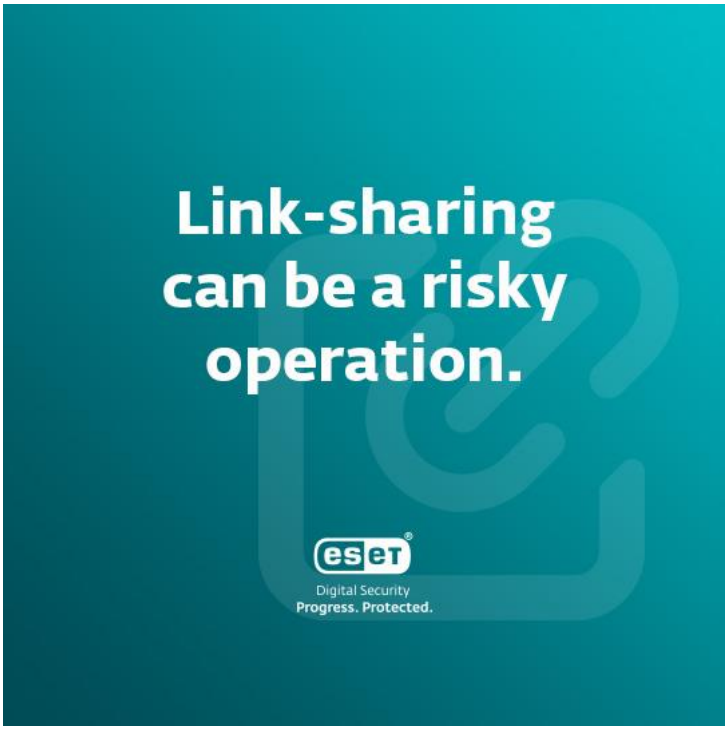



## Don't delay any updates.

If a pop-up window with a request to update your apps or software surprises you, don't hesitate to reach out to the IT department. Using an outdated version of an app or software can pose an unnecessary security risk to your safety. As an added measure, IT specialists need to check whether the newest versions remain as secure as the older versions were.


Only use designated channels for work-related communication.

When it comes to work communication, its contents may vary from sharing a sensitive document to asking your colleague whether they want to meet for lunch. In each case, however, there are appropriate channels that you can use, which have been picked based on their level of security. By using non-approved apps, you might end up with your messages and documents becoming accessible to people outside your job, endangering your company via possible data breach. Make sure that you know which sites and apps you can use for communication, and if you find yourself unsure, don't hesitate to talk to your IT specialists.



Link-sharing can be a risky operation.

Need to share a sensitive document with your colleague? Rather than creating a public sharing link, enable access directly to the people you have chosen and who have verified their identity. Ideally, opt for time-limited access if you are sharing files with someone outside your organisation. Also, sharing work-related materials to private email addresses is a no-no. Why, you ask? To minimise the risk of letting any information get into the wrong hands.


Ask your IT specialist(s) for help.

Wondering what to do when you receive a suspicious email? Not sure how to safely share a document with your colleagues? No question is stupid, so don't be afraid to ask the specialists from your IT department. Don't worry about wasting their time – your responsibility and precaution might actually save them a lot of time and trouble in the long run. It's always better to stay informed and safe than to face some more serious issues and deal with the consequences.