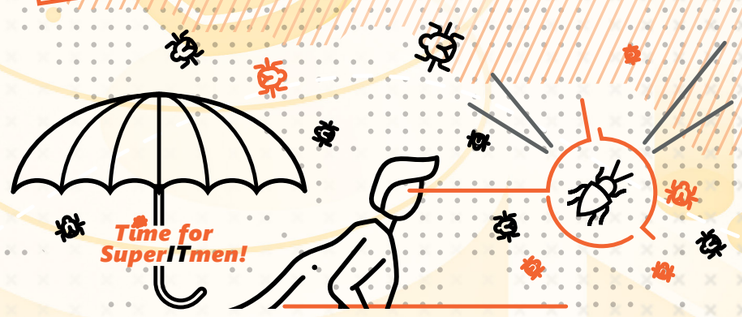
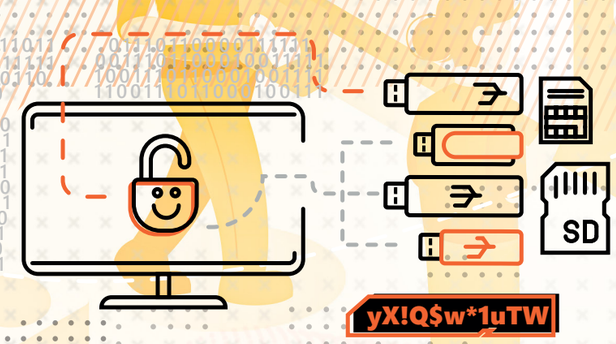
9 SECURITY TIPS FOR WORKING REMOTELY



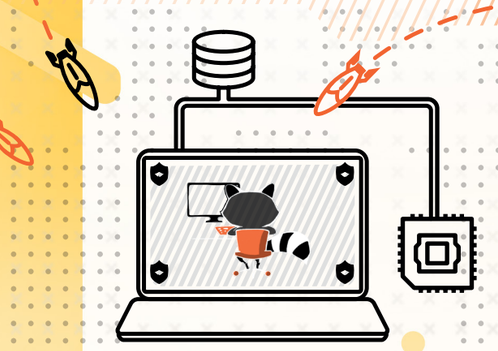
1 There are always some IT knights in the company!

If you have any doubt or something seems to you suspicious, **you should definitely ask those heroes for advice** (even if it seems to be basic knowledge). Remember – they are here to help you, even if they require a password change again...



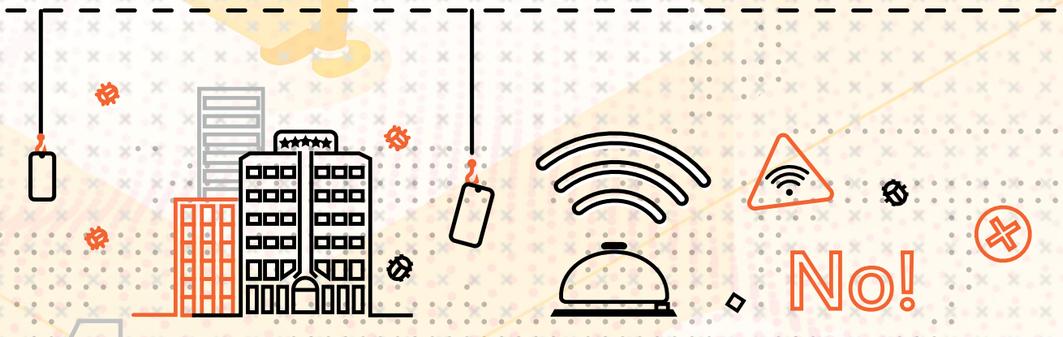
2 Secure your memory stick with a password!

By this process, you will comfortably save the data from being misused by others. **Whenever you insert the USB into a computer, a password will be required to access it**. To encrypt such storage media, you can use free tools such as VeraCrypt or BitLocker.



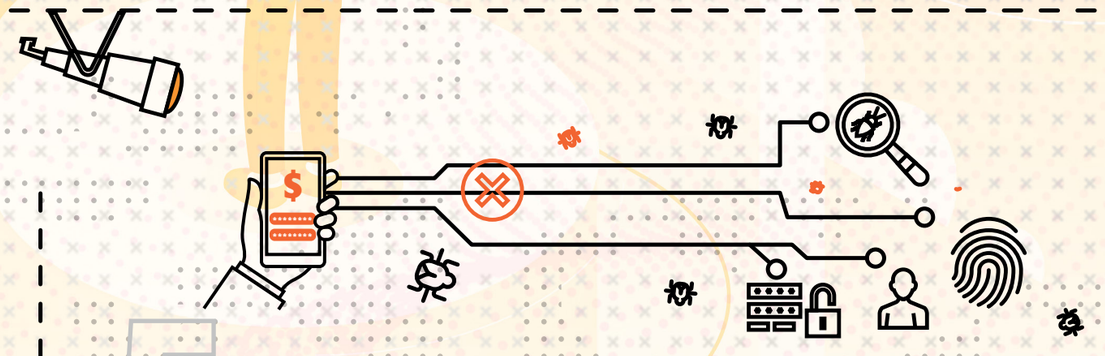
3 Protect your laptop, like a Raccoon is protecting its baby!

Never leave your laptop unattended, neither in a closed car nor even in a hotel room! Take the raccolest Computer with you or, if there is such a possibility in a public place, leave it in a safe. According to the GDPR the most expensive **corporate laptop loss can cost €20 million or 4% of the company's annual global turnover**.*



4 Avoid using public or hotel Wi-Fi networks!

If you can't use Data SIM card and **need to connect to a public/hotel wi-fi network, do it by using a trusted VPN**! This is to increase security through additional encryption. When the system asks what network you are in, answer: "public/untrusted" or if you want to "find PCs, devices, and content on this network", answer "no" - also at home.

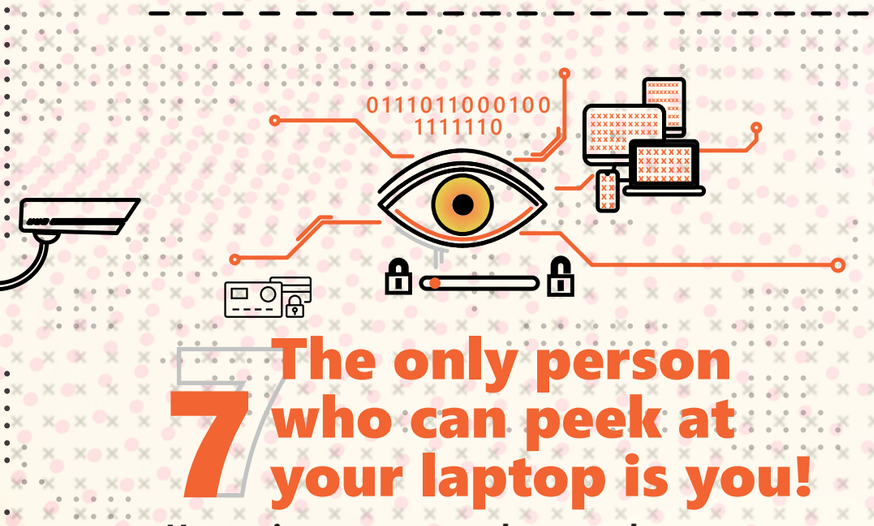


5 Don't access the bank app when connecting the public Wi-Fi!

Keeping your personal details safe is your responsibility - **make sure your data is always safe.** Never access your banking account or conduct finance--related operations through an unsecured wireless network. **Captured information can be used by hackers** to gain access to your personal accounts directly or be sold to third parties.

6 Encrypt your computer's entire disk!

If a laptop is lost or stolen and your data aren't encrypted, cybercriminals can easily intercept your sensitive data. If you go one step further and use the TPM (Trusted Platform Module) to enhance computer security and privacy – make sure you set up an authorization value such as a PIN. **In 2019 there have been 67,500 attacks on the personal data of mobile device users**!**

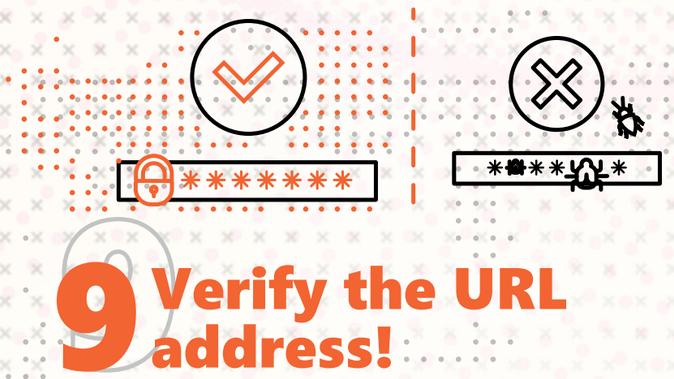


7 The only person who can peek at your laptop is you!

Use privacy screen always when you are in public or open space and keep your private and confidential information out of the eyes of strangers. While you put a privacy screen over your computer's display, you will still be able to view your screen in either orientation, but people to the left and right of you will see only a black screen.

8 Enter passwords only where there are no observers present!

When you are in a public place and entering your username/password, **a monitoring camera could capture both your screen and your keyboard**. It could be fairly straightforward for a viewer to grab or guess your credentials from the footage. If necessary, try to pretend to press a few buttons in addition to your password.



9 Verify the URL address!

Take a look at spelling and whether the connection is secure. How? **Did you notice that there is a locked padlock near the URL**? If so - it means that the website is secured. It is very important in particular when you are using your password, credit card, and all your personal information.

A safer workplace starts NOW.

* *https://www.itgovernance.co.uk/dpa-and-gdpr-penalties*

** *https://securelist.com/mobile-malware-evolution--2019/96280/*

CQURE ACADEMY