Handling Data Securely

1

Data and documents are everywhere:
Practice your cybersecurity skills!

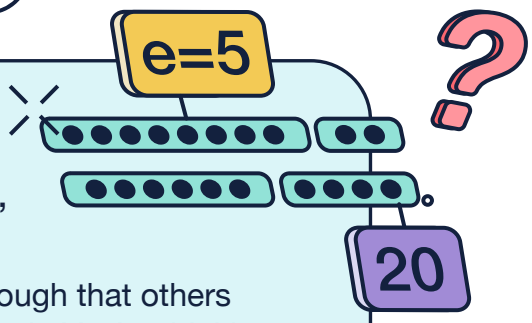
People sometimes make mistakes — some smaller, some bigger — and that's why we need to look at things in the workplace from a cybersecurity perspective. Sometimes important documents are left on a desk or by the printer. Perhaps there's a private USB stick in the computer that the IT department doesn't know about. Maybe you have a Post-it note on your monitor with your password written on it? Think about it — are your cybersecurity skills up-to-date?

2

What is the need-to-know principle?

A need-to-know principle means that access to files is only granted to the employees who require access for their job. This is especially applicable to sensitive data. Anyone who wants to access data needs both authorization and a reason for the data to be released. This means that your organization can regularly check that those who use the data are also those authorized to access it.

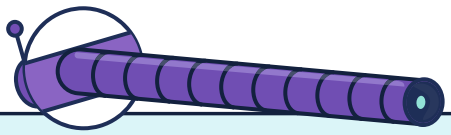
3



Passphrases are more secure than passwords. They contain several entire words, numbers, and special characters.

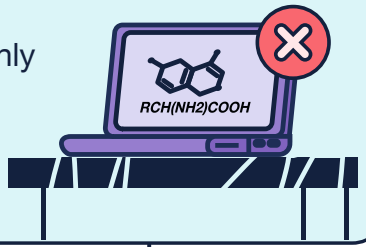
What makes a secure password? It should be complex enough that others can't guess it, but you should be able to remember it yourself. You're thinking that's not so easy? Passphrases, i.e. entire sentences where the initial letters or parts of words are put together to make up your password, can be helpful. You probably know a poem, a line from a song, or another phrase that you can easily remember. This makes for an excellent personal password when used together with numbers (such as the date the song or poem was released, or the writer's date of birth) and special characters. You are probably already aware that the name of your first pet or your significant other does not make a good password. Passwords that use personal information are easier to crack.

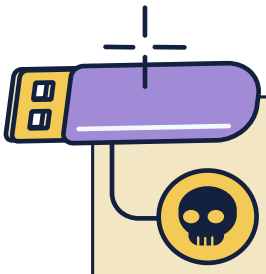
4



Documents are only as secure as the place in which they are stored.

Are files spread across your desktop in lots of folders? Or stored on your private USB stick? Bad idea! Only store documents in designated project folders, and only use storage devices provided by your organization. It is not only digital documents that are of interest to criminals. Physical documents containing sensitive information should not be left on your desk or by the printer, either.





5

Do not use private or third-party devices, cloud storage, or email services.

Saving a business document on your own cloud service to continue working on it at home might seem convenient, but don't do it! Only use the systems and equipment provided by your organization when working from home. Private laptops and smartphones always pose a security risk, as do private email services. Ideally, your organization will ensure you have equipment that allows you to work from anywhere in accordance with data protection requirements.

exploqii