Ransomware

Don’t let it cost you.

If your organisation or device gets infected with malicious software, the cybercriminal responsible for the attack can encrypt your data and block your access to it until an amount of money is paid.

System Infected → Data Locked → Payment Demanded

This is called a ransomware attack. Ransomware can cause a lot of damage in a short amount of time.

How can you get infected?

Be aware of the dangers that lurk in phishing emails and malicious websites.

Phishing emails

Don’t open attachments or click on links in emails that you aren’t expecting.

Malicious websites

Only visit websites you trust. Avoid clicking on pop-ups.

We must do whatever we can to ensure we do not fall victim to this kind of cyberattack. Protect yourself by taking the following actions:

- Keep security, browser plugins and all other software up to date.
- Ensure you have the latest version of your antivirus software installed and activated.
- Make sure you use a firewall.
- Back up your files regularly.

Never pay the ransom.
If you think you have been infected with ransomware, disconnect from the network and notify IT immediately!

Small actions can make a big difference. Take a **moment** to think about your **cybersecurity**.

KEEP YOUR ORGANISATION SAFE