Malware

What:

There are several ways malware can be downloaded onto a victim's device:

- Phishing – attackers aim to trick targets into opening an attachment loaded with malware, or into visiting an infected website
- Remote desktop protocol – hackers brute-force passwords to gain access as an admin
- Drive-by downloads – downloads which take place without the victim's knowledge upon visiting an infected website
- USB & removable media – cybercriminals load a USB with malware, leave it lying in plain sight and wait for a victim to pick it up and use

Remember, malware can:

- Lock a device or render it completely unusable
- Tamper with data or take control of accounts
- Spy on your daily activities through keylogging

What should you do?

1. Disconnect infected devices
2. Disconnect from the internet
3. Reset your credentials
4. Wipe infected devices
5. Ensure backups are free from malware before restoring
6. Connect devices to a clean network
7. Install, update and run anti-virus software
8. Reconnect to your network