



## **Types of cyber threats**

### **Identity theft**

A type of fraud that occurs when someone obtains and uses the identifying information of another person without their permission. This can include stealing the credit card number or bank account information of an individual.

### **Malware**

Malicious software that can infect your computer. It can be used for personal gain or to cause damage to the computer.

### **Ransomware**

A type of malware that restricts access to a computer system or network until a ransom is paid. It typically arrives as an email attachment and creates a lock screen with instructions for the user to follow.

### **Data breach**

When an unauthorised person gains access to sensitive personal or proprietary information. A data breach can have serious consequences for a company, such as identity theft and financial loss.

### **Trojan horse**

A type of malware that is often used to gain access to data on a computer or network. They typically exploit security vulnerabilities to enter the computer system.

### **Spyware**

Software installed without the knowledge or consent of the user. It can be installed remotely and has features that allow it to collect sensitive data from a computer.

### **Phishing and spear-phishing**

This is the practice of sending an email that appears to be from a legitimate source to steal confidential information. Spear-phishing is a more advanced form which targets specific individuals. Spear-phishers use personal information about their intended victims to make their emails more believable.

### **Denial of service**

Prevents legitimate users from accessing or using a computer or network. The attacker uses the resources of their own computer or network to flood the victim's system with more traffic than it can handle, usually with the goal of making it unusable.