UNAUTHORISED ACCESS

Access to networks by users who are not permitted to access them is called unauthorised access.

Unauthorised users can attempt to gain access to networks directly by themselves. Alternatively, they may create software that runs thousands of times per second on devices, inputting multiple login details in order to attempt to gain access to networks with poor security.

DID YOU KNOW?

In 2012, a survey showed that 31% of people store financial data on their PC.

SUBJECT VOCABULARY

malware (**mal**icious soft**ware**) software that is created with the intention to do harm

Sometimes, devices on a network can be targeted by unauthorised users in order to be used as botnets. Botnets are groups of computers that have their resources used for harmful purposes, such as running and spreading **malware**.

DELIBERATE DAMAGE BY MALWARE

Malware can show messages, play sounds, delete files or reprogram systems to perform tasks that will harm the system and the connected hardware.

SKILLS
INTELLECTUAL INTEREST AND CURIOSITY
PERSONAL AND SOCIAL RESPONSIBILITY
SELF-DIRECTION
CRITICAL THINKING
COMMUNICATION
INTERPERSONAL SKILLS

ACTIVITY

▼ THE IMPACT OF MALWARE

Research Stuxnet malware and the damage that it caused to nuclear facilities in Iran. Discuss your findings with your class.

Some malware (known as **ransomware**) threatens to delete a user's files or places restrictions on a user's access to software or resources until money is paid, usually to an anonymous account. These messages are usually very threatening and distressing for users. They are often written in a way that makes the user believe that they must pay quickly. This puts pressure on the user to act before they have time to think clearly about the threat and how to manage it.

▲ Figure 6.2 Ransomware

ACCIDENTAL DELETION

Users can sometimes delete files or even the entire contents of a drive by mistake. This can happen if:

- they press a key on a keyboard by accident
- they format media on the wrong storage device
- their device loses power unexpectedly.

THEFT OF PERSONAL DATA

Criminals use a number of methods to steal personal data.

SUBJECT VOCABULARY

phishing the criminal activity of sending emails or having a website that is intended to trick someone into giving away personal information such as their bank account number or their computer password; this information is then used to get money or goods

PHISHING

Phishing is a technique used by criminals to get personal information and payment details from users. It involves sending large numbers of messages that appear to be from real organisations, such as shops, banks or charities. Phishing messages are often sent as emails. These emails ask the user to provide their information by replying to the message or following a hyperlink that opens a webpage into which the user is asked to type their personal details.

Compliments of the season

I am the Head of Corporate Investment at Investments and Securities Dubai.

I do have an authorisation of a client who is an African leader with difficult political position to seek for individuals with financial management understanding to handle his wealth devoid of his name.

If you have experiences or projects in need of funding do let us have a description of your experiences alongside your address and business name so we can discuss a lot more.

Sincerely

Mukhtar Hassan

▲ Figure 6.3 Some phishing emails are less believable than others; the email address can be a giveaway as to the authenticity of the sender

Sometimes, phishing messages are highly customised or personalised and are targeted at a smaller number of particular users. This technique has become known as spear phishing.

DID YOU KNOW?

The threat from spear phishing grew by 55% between 2014 and 2015.

DID YOU KNOW?

SMS phishing is sometimes referred to as smishing.

Phishing messages can also be sent via SMS or instant message apps so that users open the fake webpage in a mobile browser. Users may not realise that the webpage is fake, particularly if they have never seen the company's real webpage in a mobile browser. As a result, they might type in their username and password details and reveal this personal data to the criminals.

▲ Figure 6.4 A fake **webform**, linked from an SMS message and opened in a mobile browser

SUBJECT VOCABULARY

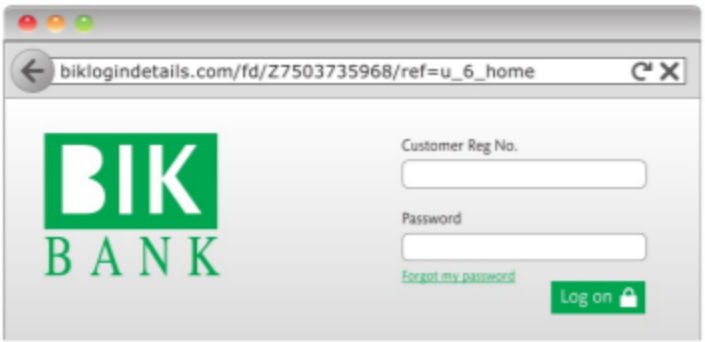
webform a data entry form on a web page
internet traffic data transferred between computers connected to the internet
domain name server a computer connected to the internet that translates domain names, such as pearson.com, into IP addresses

PHARMING

Like phishing, pharming is a technique used by criminals to gain personal information and payment details from users. Criminals create fake versions of trusted websites to trick users into entering their login details, which are then used by the criminals to access users' accounts.

There are two main methods by which users are directed to a pharming site.

- **Internet traffic** going to the real website is redirected to the fake website, so that users think they are visiting the real thing. Criminals do this by altering the **domain name servers** to make internet traffic go to their fake site. They can also use malware to redirect web requests.
- Often, the URL of a pharming website is designed to be very similar to the URL of the real website. This means that if a user misspells the URL when typing it into the address bar of their web browser, they could go to the pharming site by mistake. For example, if the URL of a real bank is http://moneybank.lk and the criminals create a website with the URL http://moneybamk.lk, it could be easy for the user to make a mistake and arrive at the fake website.



▲ Figure 6.5 Users should always check the URL of websites that they visit to make sure that they are not fake websites

METHODS TO SECURE DATA AND PERSONAL INFORMATION ONLINE

Much of the data transmitted online is sensitive and valuable, and it is important to protect that data from unauthorised access. There are several different methods used to secure data and personal information.

FIREWALLS

Firewalls control the data travelling into and out of a network. They examine the network addresses and ports of the data. They then compare those details to a list of rules that can be changed by network administrators. The list of rules determines what traffic should be allowed to travel into and out of the network. In this way, firewalls can prevent unauthorised access to a network and protect the network from malware. See *Unit 2 Connectivity* (page 90) for more information about firewalls.