Learning Objectives

- Define what is meant by the term ‘cyberattack’
- Describe the financial, reputational and legal damage that a cyberattack can cause
- Describe the characteristics of and threat posed by different types of malware
- Describe how anti-malware works
- Explain why it is important to keep anti-malware up-to-date
- Define what is meant by the term ‘social engineering’
- Describe commonly used social engineering tactics (phishing, pretexting, baiting, quid pro quo) used by hackers

Twitter under attack

In mid-July 2020, a number of high-profile verified Twitter accounts were breached. Accounts associated with Barak Obama, Jeff Bezos, Bill Gates, Apple and Uber all posted similar tweets instructing people to send bitcoin to the same account. The tweets were removed, but they continued to be posted throughout the day.

For a day, verified accounts were unable to post tweets as Twitter investigated the attack.

Cyberattack

The news story we have just read is an example of a large scale **cyberattack**.

Cyberattacks are malicious acts in which a computer system comes under attack by unauthorised persons, who are generally known as hackers.

Why might people launch such attacks?

Financial and reputational damage

- WannaCry was a **ransomware** attack that affected hundreds of organisations in 2017. The National Health Service (NHS) suffered an estimated £92-million loss as a direct result of the attack.
- The NHS also suffered damage to its reputation.
- WannaCry is a known vulnerability that required a patch to fix.
- Microsoft released the patch, but many NHS trusts did not implement it.
- This meant that they were vulnerable to the attack.
- When this came to light, many people were concerned about the lack of up-to-date software within the NHS.

Ransomware case study (WannaCry)

Legal damage

Attacks of this nature can have legal implications for the organisations that are impacted by them.

In May 2020, the airline easyJet came under attack, when the email addresses and travel details of approximately 9 million customers were stolen. More than 2,000 customers also had their credit card details stolen.

In June 2020, over 10,000 people joined a class-action lawsuit against easyJet in an attempt to get compensation for the loss of their data.

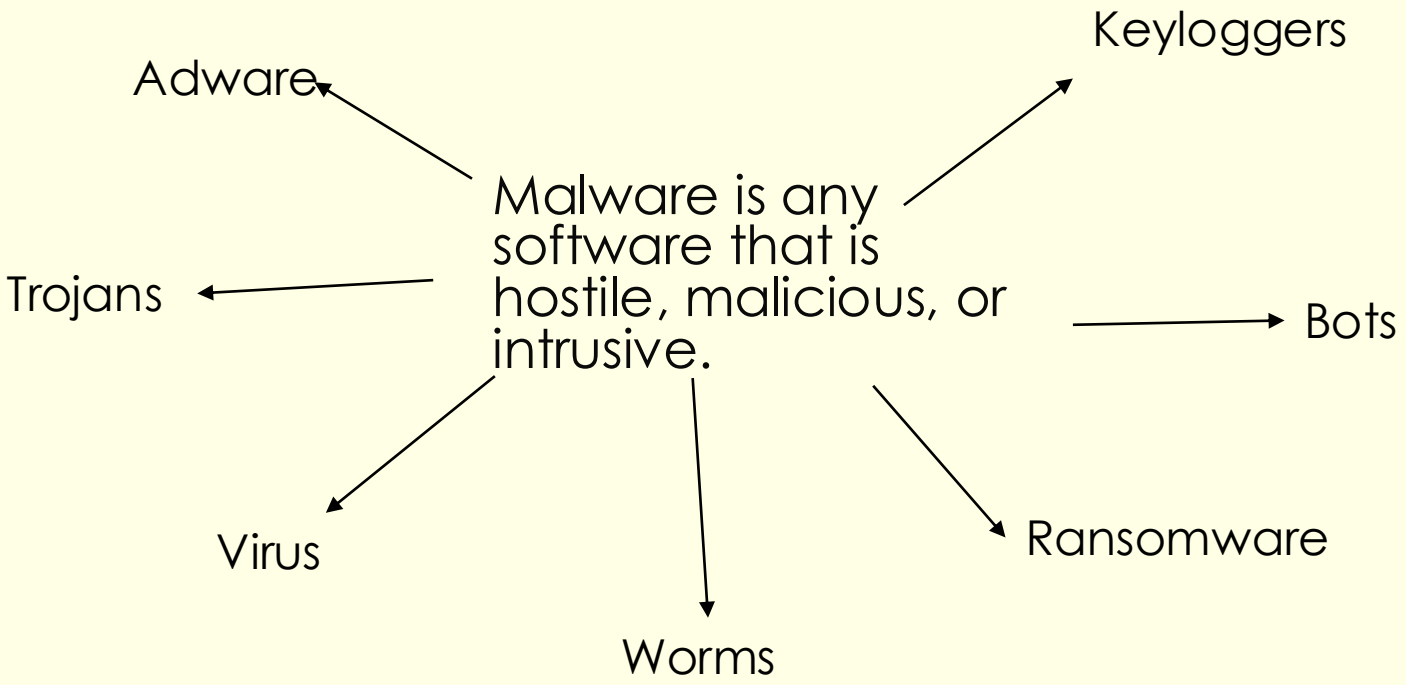
Targeting information

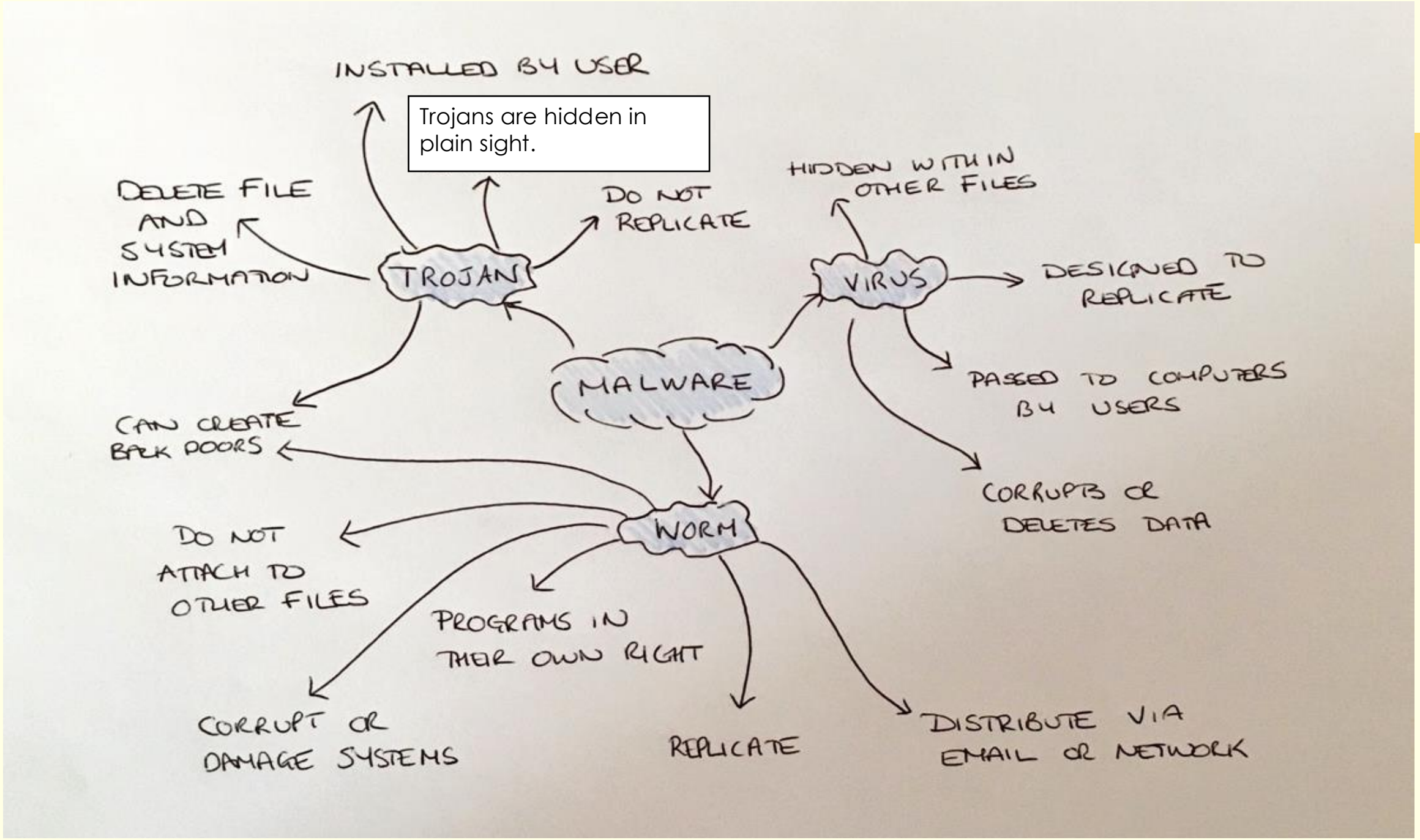
Often the purpose of cyberattacks is to steal information. This is usually data such as email addresses and credit card details. This information is often used for further crime such as identity theft or fraud.

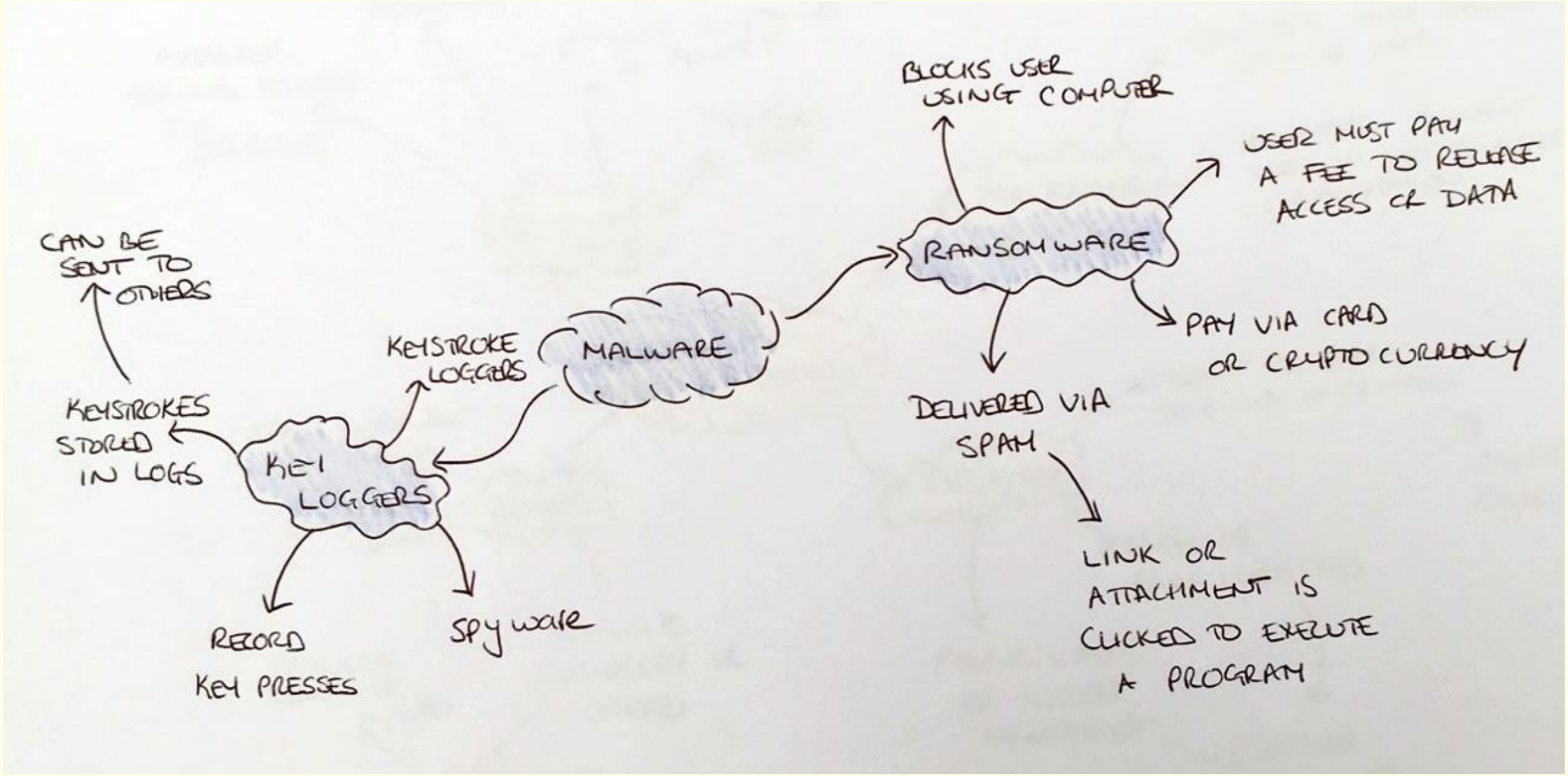
Information that is stolen might also comprise intellectual property, such as source codes or patented designs that can be sold on the black market.

Sometimes data is encrypted (using ransomware attacks) in order to damage an organisation financially or reputationally.

What is malware?




INSTALLED BY USER
Trojans are hidden in plain sight.
DELETE FILE AND SYSTEM INFORMATION
DO NOT REPLICATE
HIDDEN WITHIN OTHER FILES
TROJAN
VIRUS
DESIGNED TO REPLICATE
MALWARE
PASSED TO COMPUTERS BY USERS
CAN CREATE BACK DOORS
CORRUPTS OR DELETES DATA
WORM
DO NOT ATTACH TO OTHER FILES
PROGRAMS IN THEIR OWN RIGHT
CORRUPT OR DAMAGE SYSTEMS
REPLICATE
DISTRIBUTE VIA EMAIL OR NETWORK


BLOCKS USER USING COMPUTER
USER MUST PAY A FEE TO RELEASE ACCESS OR DATA
RANSOMWARE
PAY VIA CARD OR CRYPTO CURRENCY
DELIVERED VIA SPAM
LINK OR ATTACHMENT IS CLICKED TO EXECUTE A PROGRAM
MALWARE
KEYSTROKE LOGGERS
KEY LOGGERS
CAN BE SENT TO OTHERS
KEYSTROKES STORED IN LOGS
RECORD KEY PRESSES
SPYWARE

Investigate the ransomware attack on Travelex in early January 2020.
Write a summary of the attack. Consider these aspects:

- What did the attack look like to Travelex?
- What individuals or organisations were affected?
- Who were responsible?
- Why did they believe Travelex would pay?
- How did Travelex respond?
- Was it an appropriate response? Why?
- What was the impact of the attack on individuals, organisations and Travelex?
- What could Travelex do in the future to avoid the same kind of attack?

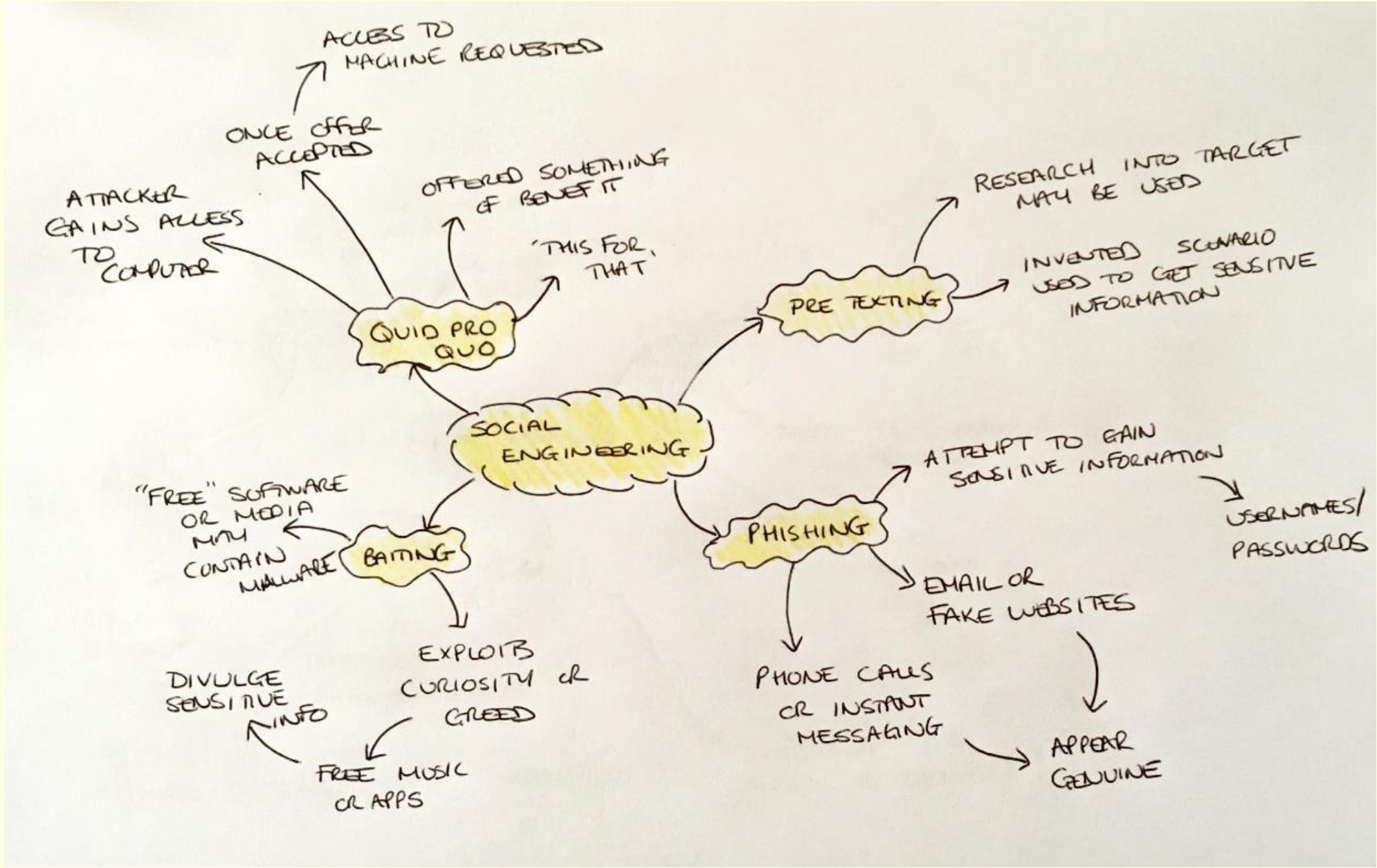
Lots of information online for this question, some good places to start are:

- bbc.co.uk – search for the article 'Travelex being held to ransom by hackers'.
- infosecurity-magazine.com – search for the article 'Why the Travelex Incident Portends the Changing Nature of Ransomware'.
- computerweekly.com – search for 'Cyber gangsters demand payment from Travelex after 'Sodinokibi' attack'.

SOCIAL ENGINEERING

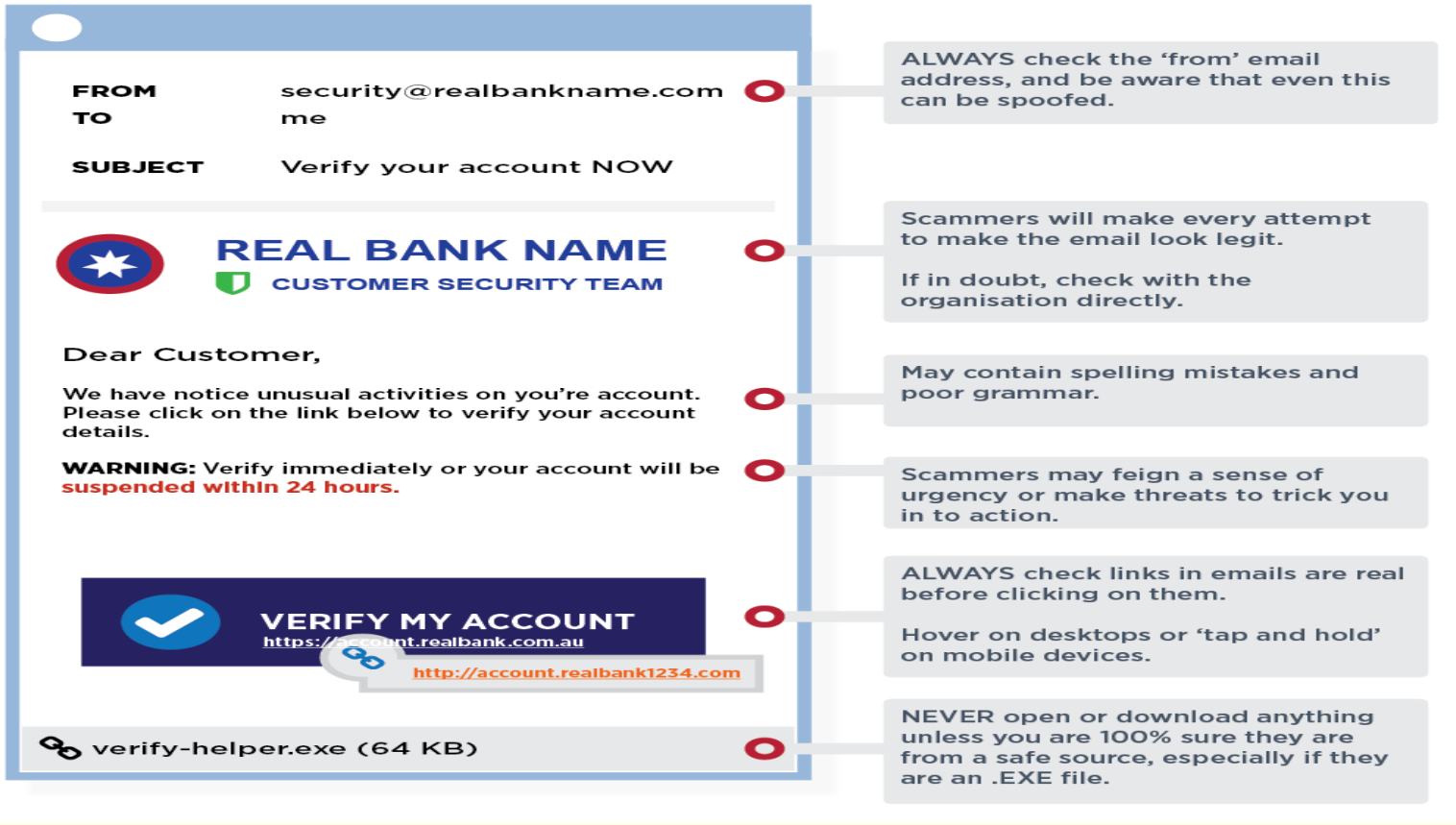
- Social engineering is a technique used by criminals to manipulate or trick people into revealing confidential information.
- The data obtained is used to gain access to a computer system.
- Social engineering is one of the most common methods used by cyber criminals.
- This is because people are generally trusting of others and this makes them a weak link where network security is concerned.

Social Engineering



Types of Social Engineering

Phishing: Phishing is **a type of social engineering attack often used to steal user data, including login credentials and credit card numbers**. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.



Baiting

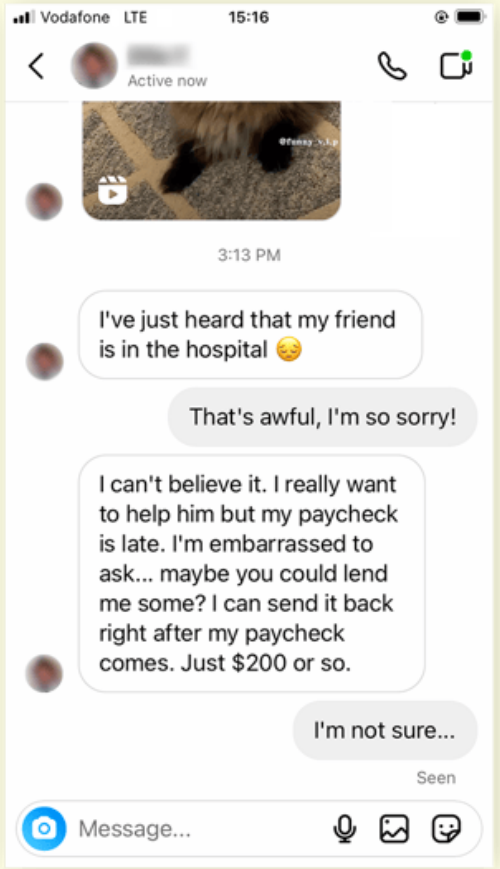
The most common form of baiting uses physical media to disperse malware.

For example, attackers leave the bait of a malware-infected flash drives in conspicuous areas where potential victims are certain to see them.

Types of Social Engineering

Pretexting

Pretexting is use of a fabricated story, or pretext, to gain a victim's trust and trick or manipulate them into sharing sensitive information, downloading malware, sending money to criminals, or harming organization they work for.



Quid pro quo

The attacker promises the victim a favour in exchange for information or other benefits.

When launching a quid pro quo attack, the attacker offers the victim some benefit.

It could be a service, such as removing malware and potential viruses from the victim's computer.

To receive the benefit, the victim must first do something – for example, give the attacker access to their computer or send them their login credentials.

Attackers may only ask for phone numbers or email addresses, but these can be used in future malicious campaigns, e.g., for phishing.

Protecting against social engineering

Social engineering attacks rely on humans making mistakes.

Protecting a system from human error is highly challenging.

One of the best defensive tools organisations can use is an **Acceptable Use Policy (AUP)**.

An AUP is a collection of rules and procedures that employees are required to follow in order to protect their organisation's systems and networks.

Training is often provided to reinforce an AUP's rules.

Social Engineering Prevention

1) Don't give up your private information
2) Enable spam filter
3) Stay cautious of your password – use strong passwords and change them regularly
4) Keep system software up to date
5) Pay attention to what you do online - Train yourself to not click on Clickbait and scam advertisements. Always know that most lotteries you find online are fake!
6) Do not click on spam links, do not open suspicious emails.
7) Only use https sites – secure websites when entering personal information

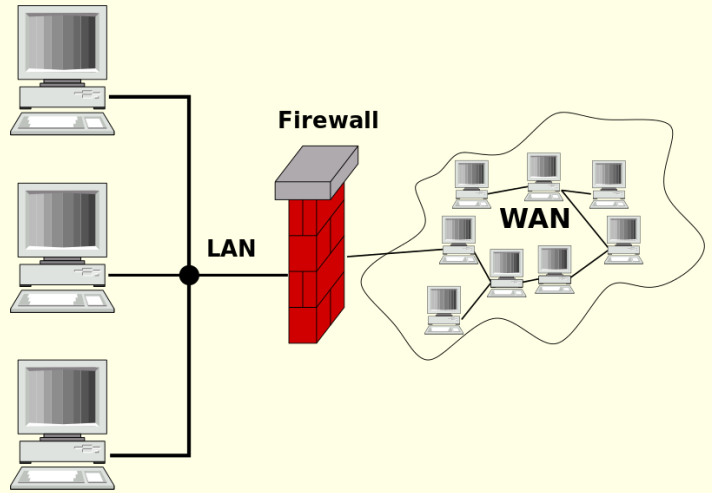
Learning Objectives

- Describe how anti-malware works
- Explain why it is important to keep anti-malware up-to-date
- Describe other ways of protecting systems and data

Recap Firewalls

Complete the sentences below with words from the following list to describe the role and function of a firewall.

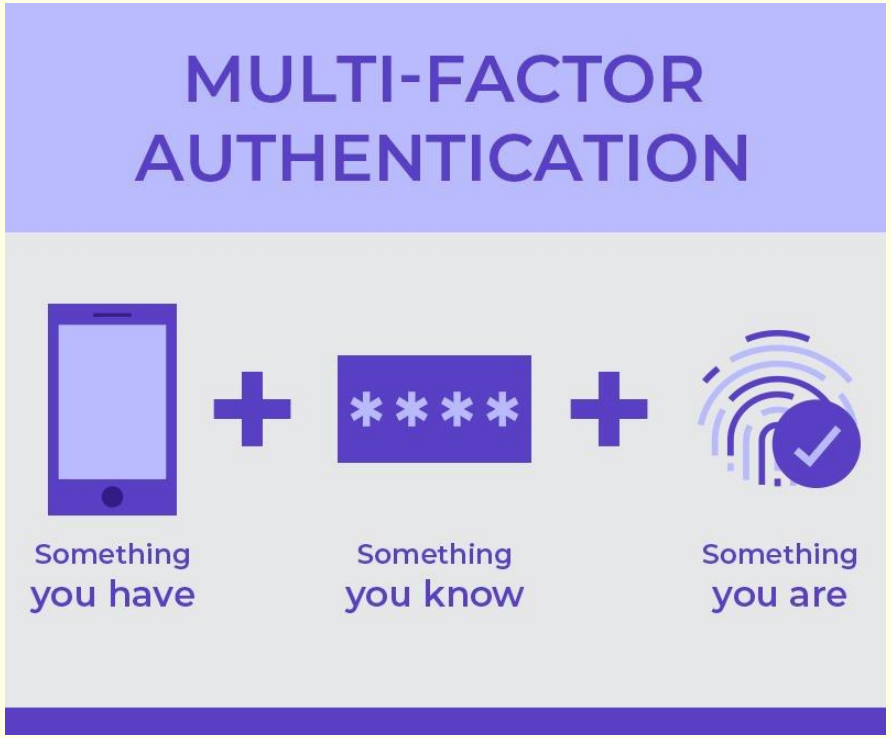
Network (LAN)	Packet	Vice versa
Monitors	Software	Logged
Discarded	Traffic	Internet (WAN)
Inside	Rules	Hardware



1. A firewall is a piece of _____.
2. It runs on a piece of _____ attached to a _____on one side and the _____on the other.
3. It _____ the network _____ between the inside and the outside.
4. The software consists of a set of _____.
5. Each network _____ moving from _____ to outside and _____has the rules applied to it.
6. Unauthorised traffic is _____and _____.

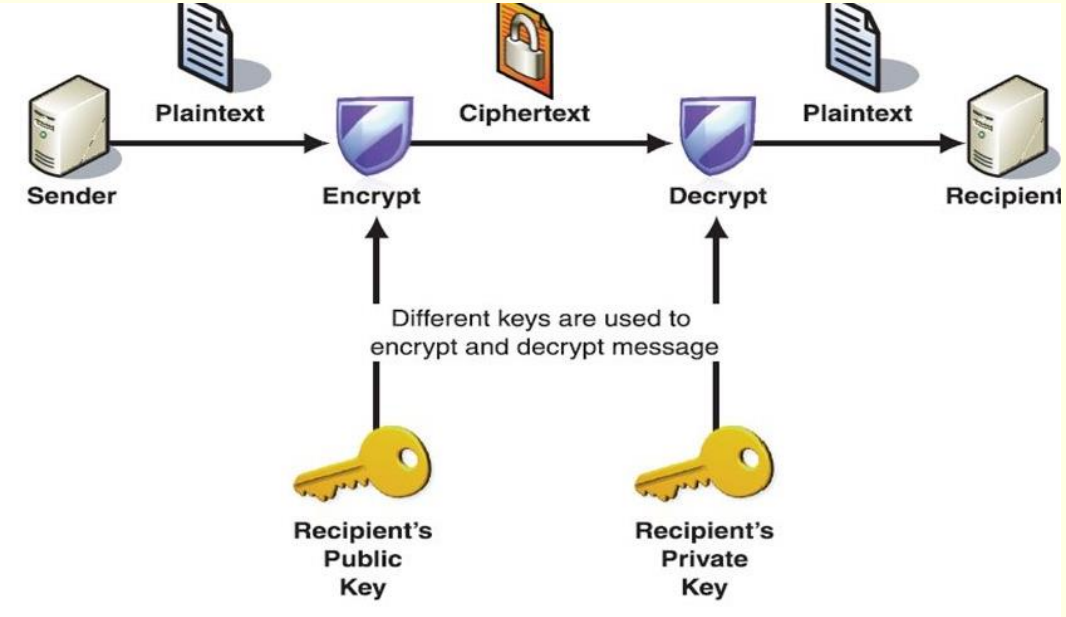
Recap: Securing Access

- Encryption
- Complex Passwords
- Limits to the number of password guesses
- Physical "keys" (key chains, swipe cards)
- Biometrics (fingerprints, retina scanning, Voice, Facial recognition)
- Two-Factor Authentication



Recap: Encryption

- Encryption is where data is **scrambled** so that if it is accessed unlawfully then it will be meaningless to the person viewing it.
- However, it does not prevent an unauthorised person from accessing the data, but it does make it almost impossible for them to understand it.
- When encryption is used, only the intended recipient of the data will be able to decipher (unscramble) the data using a decryption key



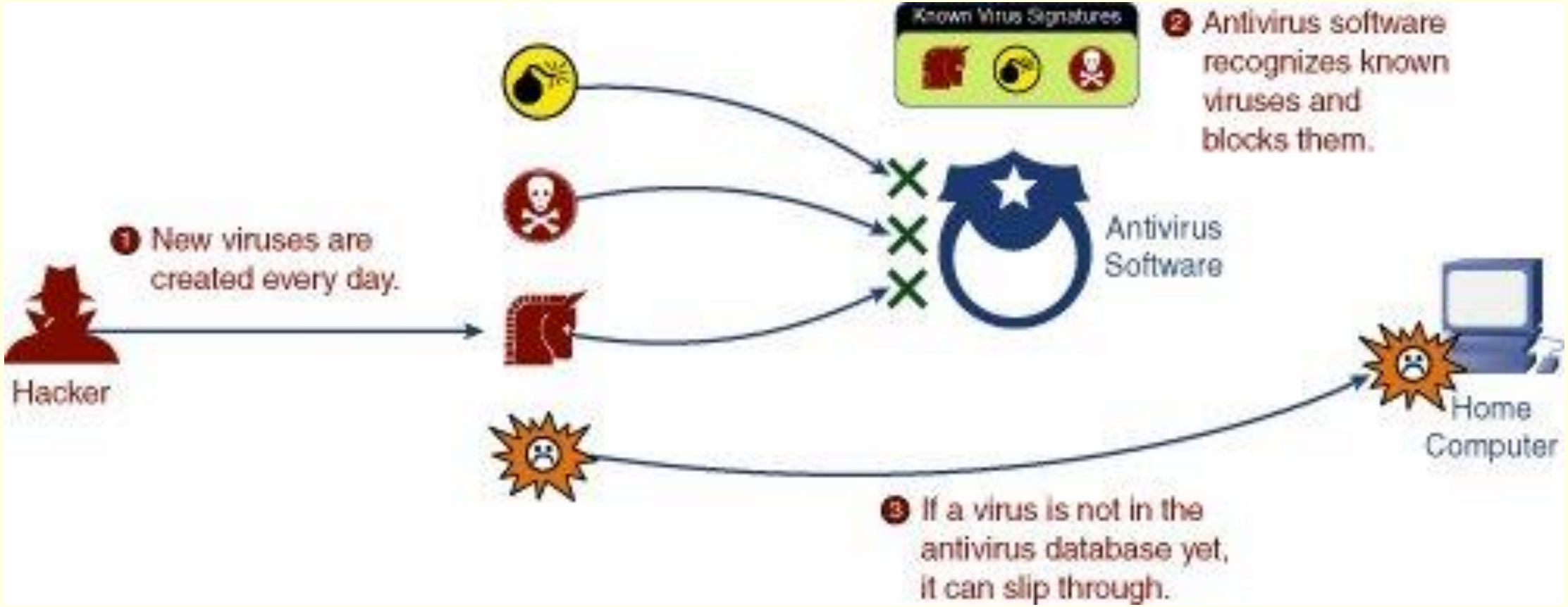
Recap: User access levels

- Allows a system administrator to set up a hierarchy of users
- Lower level users would have access to limited information and settings
- Higher level users can access the most sensitive data on the system
- Preventing users from accessing/changing certain parts of the system and files if they do not have the access rights

How to protect against attacks

- keeping **software up to date** using patches to fix security issues
- considering replacing software that is no longer supported by the creator, which may be vulnerable in the future
- **installing anti-malware software** that either:
  - scans for malware using **signatures**
  - signature files are databases
  - signature files, themselves, must be kept up to date
  - detects malware using **heuristics**
  - should also be updated to ensure the use of latest knowledge about malware
- ensuring that anti-malware is scanning downloads from the Internet
- ensuring that anti-malware can, if required, scan portable devices attached to the computer
- Regularly back-up data

Virus Detection Using Known Virus Signatures



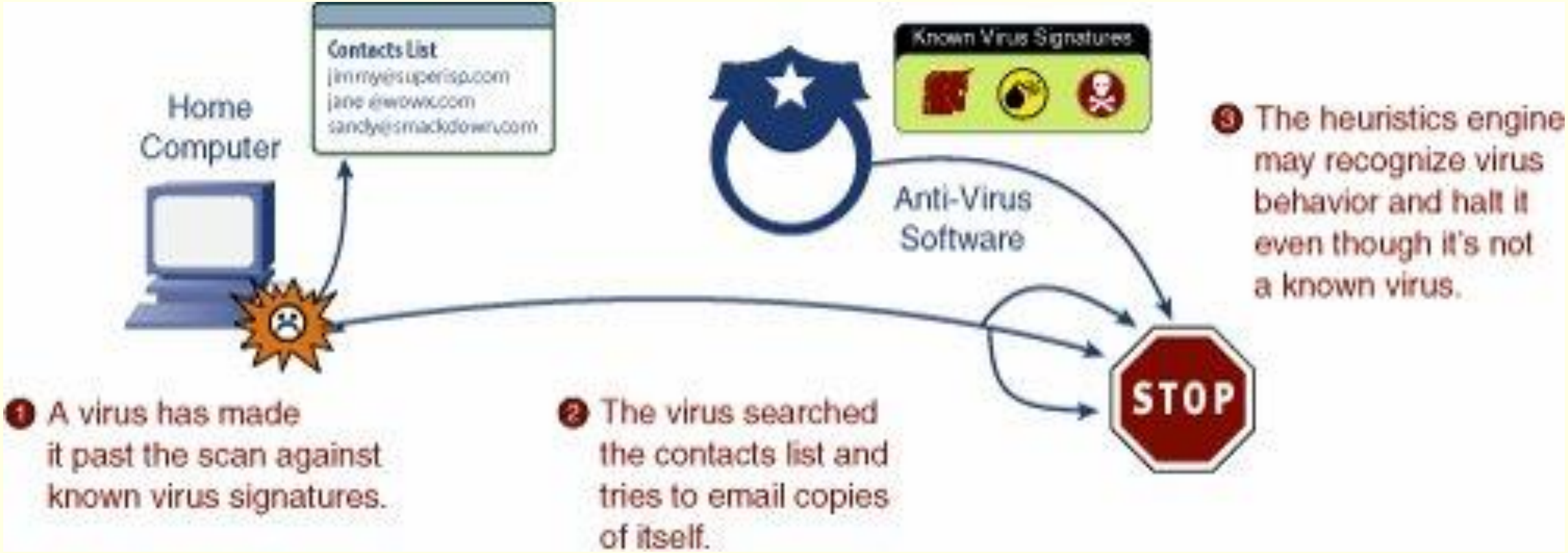
Heuristic analysis

Anti-malware programs can only work with information that is already known about malicious programs.

However, new malware is being created all the time to exploit different vulnerabilities.

Heuristic analysis is a scanning technique used by many antivirus programs - they look for certain malicious behaviours from potentially new and undetected variants

Heuristic analysis



Exam Style questions – anti-malware

1. State two ways that anti-malware software may identify an infection. (2 marks)

2. Explain why users should always apply patches to their software. (2 marks)

3. Describe the role of a signature file in anti-malware software. (2 marks)