

Cyber security

Read online at pastopic.com/cambridge/computer-science-0478/notes/cyber-security

Last checked 30 September 2026

Read first: [The internet and the world wide web](#), [Encryption](#)

© 2026 Pastopic. Free for personal study. Please share the link, not the file.

What you need to know

By the end of this topic you should be able to:

1. **Describe how each of these threats is carried out and what the attacker is trying to achieve:**
 - a **brute-force attack** (guessing a password by trying combination after combination);
 - **data interception** (capturing data while it travels across a network);
 - a **distributed denial of service (DDoS) attack** (flooding a server with requests from many computers);
 - **hacking** (getting into a computer system without permission);
 - **malware: virus, worm, Trojan horse, spyware, adware and ransomware**;
 - **pharming** (secretly redirecting a user from a real website to a fake one);
 - **phishing** (a genuine-looking email that lures the user to a fake website);
 - **social engineering** (tricking people, rather than computers, into giving something away).
2. **Explain how each of these solutions helps keep data safe:**
 - **access levels**;
 - **anti-malware**, including **anti-virus** and **anti-spyware**;
 - **authentication**: a **username and password**, **biometrics** and **two-step verification**;
 - **automating software updates**;
 - **checking the spelling and tone** of emails and messages;
 - **checking the URL** a link really points to;
 - **firewalls**;
 - **privacy settings**;
 - **proxy servers**;
 - the **SSL (secure socket layer)** protocol.

How encryption itself works (symmetric and asymmetric keys) is in the encryption note; how a web page is fetched is in the internet and world wide web note. Accidental data loss (power cuts, deleting files by mistake) was asked about in 2021–2022 but is **no longer in the syllabus**.

Understand it

Threats and why people carry them out

Every threat has a **process** (what the attacker actually does) and an **aim** (what they want). Exam answers need both, and the process must be a chain of steps, not just the threat's name.

Most attacks have one of a few aims: to **steal** personal data (bank details, logins, identities) to use or sell; to **delete, change or lock** data; to **stop a service** from working; or to **damage an organisation's reputation**, sometimes to demand money to stop.

Brute-force attack

A **brute-force attack** is **trial and error**: the attacker tries one password after another, **over and over**, until one works. It can be done by hand, but usually **software** tries thousands of combinations a second automatically, starting with common passwords and words.

Why length and variety matter: a 4-digit PIN has only $10^4 = 10\,000$ possibilities, so software trying 1000 a second gets through all of them in 10 seconds. An 8-character password using lower-case letters, capitals and digits (62 characters) has $62^8 \approx 2.18 \times 10^{14}$ possibilities; at the same speed that is about 6900 years.

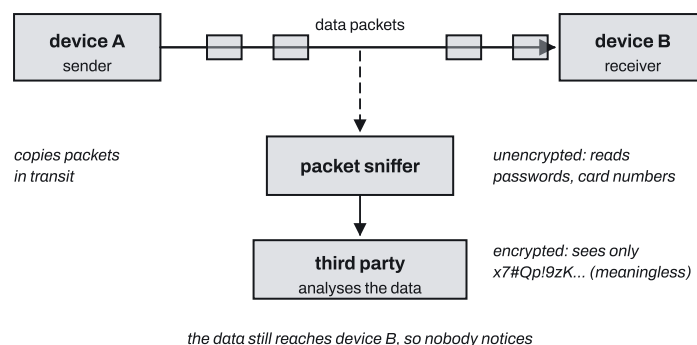
Aims: once in, the attacker can **view or steal** data, **delete or change** it, **lock the owner out** (or encrypt the data), **install malware**, or **damage the organisation's reputation**.

Hacking

Hacking means **gaining unauthorised access** to a computer or system: getting in without permission, for example by exploiting a weakness in software or by using a stolen or guessed password. A hacker can then **read, copy, change or delete** data, or plant malware. Hacking often uses other threats (brute force, spyware) but is not itself malware.

Data interception

Data sent over a network travels as **packets**. In **data interception**, a third party **captures the packets while they are in transit** between sender and receiver, often with a **packet sniffer** (software that examines packets as they pass) or by listening in on a wireless network. The captured data is sent on to the attacker, who **analyses** it for anything useful, such as passwords or card numbers. The sender and receiver usually don't notice, because the data still arrives.

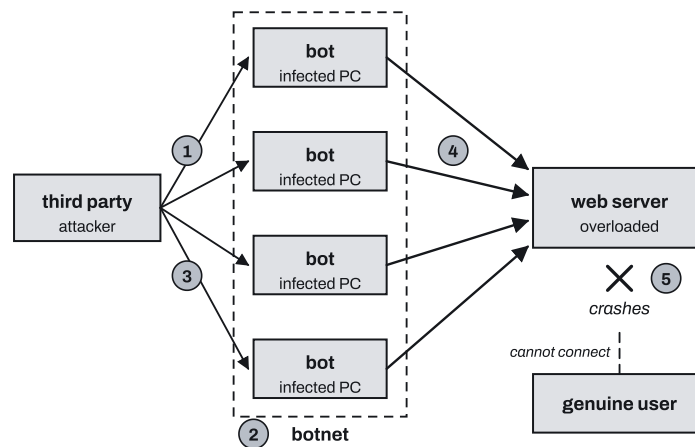


The fix is **encryption**: intercepted data is **meaningless** to anyone without the decryption key. Interception is not prevented, but it becomes useless.

DDoS attack

A **denial of service** attack floods a **web server** with so many requests that it cannot cope, so it slows down or **crashes** and **genuine users can't reach the website**. In a **distributed** DoS the requests come from **many computers at once**, which makes it far bigger and much harder to block:

1. The attacker spreads **malware**, which users download without realising.
2. The malware turns each infected computer into a **bot** (a "zombie" the attacker can control).
3. Together the bots form a **botnet**.
4. When the attacker **starts the attack**, every bot sends requests to the target **web server at the same time**.
5. The server is overwhelmed and **crashes**, so legitimate requests can't get through.



1 malware sent to PCs · 2 PCs become bots, forming a botnet · 3 attack started
4 all bots send requests at once · 5 server crashes; genuine users locked out

Nothing is installed **on the web server**: the malware is on the bots, and the server is just the target. **Aims**: revenge, damaging a company's reputation, demanding a **ransom** to stop the attack, entertainment, or testing how well a system copes.

Malware

Malware is **malicious software**: any program written to cause harm. Learn the six types and what makes each one different.

Malware	What it does	Key feature
Virus	Copies itself into other files and programs; damages, deletes or corrupts data	Needs a host : it only spreads when the infected file is run
Worm	Copies itself from computer to computer across a network ; uses up bandwidth; can carry other malware	Spreads by itself , with no host and no user action
Trojan horse	Looks like genuine, useful software; when installed, it installs the malware hidden inside it	Disguised as something wanted
Spyware	Records what the user does, especially key presses (a keylogger), and sends the data to a third party , who analyses it for passwords and card numbers	Watches and reports
Adware	Shows unwanted adverts , often pop-ups; may redirect searches to other websites and slow the computer	Advertising
Ransomware	Encrypts the user's files (or locks the computer) and demands payment for the key	Holds data to ransom

Phishing and pharming are not malware, and neither is hacking. Phishing is an email trick; hacking is an act of getting in. (Pharming *uses* malware, but the threat is the redirection.)

Phishing and pharming

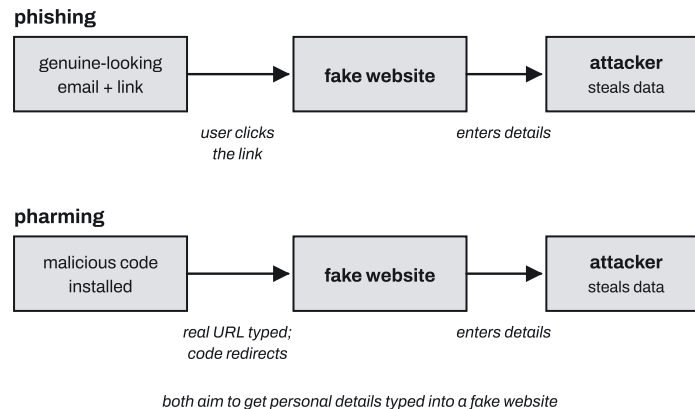
Both aim to get a user to **type personal details** (logins, bank details) into a **fake website** that looks like the real one. They differ in **how the user gets there**.

Phishing:

1. The attacker sends an email (or message) that **looks legitimate**, for example from a bank or delivery company.
2. The user **clicks a link** in it (or replies to it). Just **opening** the email does nothing: the click is what matters.
3. The link takes them to a **fake website**.
4. They enter their **personal details**, which the attacker **collects and uses**.

Pharming:

1. **Malicious code** is **installed** on the user's computer without them knowing (for example from a download or an attachment).
2. Later the user types the **genuine URL** of a site, or uses a bookmark.
3. The code **redirects** the request to a **fake website** instead.
4. They enter their details, which are stolen.



Pharming is harder to spot, because the user did everything right. Checking the URL in the address bar and looking for HTTPS and a valid certificate still helps.

Social engineering

Social engineering attacks the **person, not the computer**: the attacker **manipulates or deceives** someone into giving away **confidential data** or into making a mistake that lets the attacker in. It works by using trust, fear, curiosity or urgency. Examples:

- **phishing** (a fake email that seems to come from someone trusted);
- **baiting**: leaving an infected USB stick labelled "Salaries 2026" where staff will find it and plug it in;
- **shoulder surfing**: watching someone type their PIN or password;
- **pretexting**: phoning someone while pretending to be from IT support and asking for their password.

Firewalls and anti-malware can't stop someone choosing to hand over a password, so the defence is **training people** to be suspicious and to check.

Solutions: authentication

Authentication checks a user is who they claim to be before letting them in.

- **Username and password**. Weak on their own if the password is short or common. A **strong password** is long and mixes letters, digits and symbols, so it is much harder to guess by brute force. Systems can also **limit the number of attempts** (lock the account after, say, 5 wrong tries), which stops brute force dead.
- **Biometrics**: a fingerprint, face, iris or voice. It is **unique** to the person, can't be guessed, forgotten or easily faked, and **nothing is typed**, so there are no key presses for spyware to record.
- **Two-step verification** (also called two-factor authentication): after the password, a **one-time code** is sent to the user's **registered device** (phone or email), and it must be entered too. A hacker who has stolen the password still can't get in without that device.

Other ways to beat spyware at login: choosing characters from **drop-down boxes** or an **on-screen keyboard** (no key presses to log), or being asked for only **some characters** of the password (for example the 2nd, 5th and 7th), so the whole password is never captured in one go.

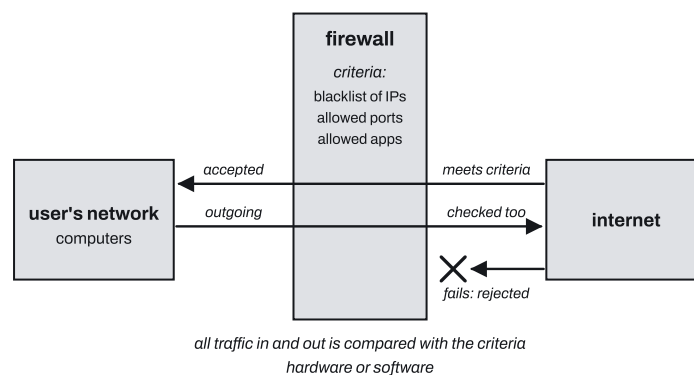
Solutions: software and checks

- **Anti-malware** (including **anti-virus** and **anti-spyware**) **scans** files, downloads and memory, **compares** them with a database of known malware, and **quarantines or deletes** anything it finds. Anti-spyware specifically finds and removes spyware, so passwords can't be captured.
- **Automating software updates.** Updates **patch weaknesses** that hackers and malware exploit, and update anti-malware's list of known malware. Making them automatic means they are installed as soon as they are released, **without relying on the user** to remember.
- **Checking the spelling and tone** of emails and messages. Phishing messages often have spelling or grammar mistakes, a generic greeting ("Dear customer"), or an **urgent or threatening tone** ("act within 24 hours or your account is closed"). Also check the **sender's email address**, which may be slightly wrong.
- **Checking the URL attached to a link.** The words shown for a link can say anything. Hover over it (or check the address bar after arriving) to see the real address: a misspelt domain (`paypal.com`), extra words (`mybank.login-verify.net`) or a missing `https` are warning signs.
- **Privacy settings** on social media, browsers and apps control **who can see** your posts, profile, location and contact details. Tighter settings mean less personal data for attackers to use for social engineering or to guess passwords and security answers.
- **Access levels** give different users **different permissions** for data: some can only **read** it, some can **edit** it, some can **delete** it, and others can't see it at all. They are set per **username**. Staff get only the access their job needs, so if an account is misused or hacked, the damage is limited.

Solutions: firewalls and proxy servers

A **firewall** sits **between a computer (or network) and the internet** and can be **hardware or software**. It **examines all traffic coming in and going out**:

1. The user or network manager sets **criteria (rules)**, for example a **blacklist** of IP addresses to block, a **whitelist** of allowed ones, or which **ports** and applications may be used.
2. Each piece of traffic is **checked against the criteria**.
3. Traffic that **meets** them is **allowed through**; traffic that **doesn't** is **rejected** (blocked), and the user can be warned.
4. It can **close ports** that hackers use and block malware trying to get in or to send data out.



A **proxy server** is an **intermediary**: requests to a web server go to the proxy first, and the proxy deals with them. It protects the **web server**:

- it **examines each request** before passing it on, and can act as a firewall;
- it can **limit the rate** of requests and **block IP addresses** sending too many, so a DDoS doesn't reach the server;
- it keeps a **cache** of frequently requested pages and **answers those requests itself**, so fewer requests reach the server (and pages load faster);
- it **hides the web server's IP address**, so attackers can't target the server directly.

Firewalls and proxy servers both filter traffic, both can hold blacklists and whitelists, both block unauthorised access, and both can be hardware or software. The difference: a **proxy handles requests on the server's behalf**, so it can **hide the IP address** and **cache pages**; a firewall only lets traffic through or blocks it.

Solution: SSL

SSL (secure socket layer) is a protocol that makes data sent between a web browser and a web server secure. Its newer version is **TLS (transport layer security)**; HTTP used with it is **HTTPS**. It creates a secure connection like this:

1. The **web browser** asks the **web server** to **identify itself**.
2. The web server sends its **digital certificate**.
3. The browser **checks (authenticates)** the certificate.
4. If it is **authentic**, an **encrypted** connection is set up (using **asymmetric** encryption) and data can be sent; intercepted data is meaningless.
5. If it is **not** authentic, the connection is **rejected** and the user is warned.

A user can tell a site uses SSL because the URL starts **https**, there is a **padlock** by the address, and they can **view the digital certificate**.

Key facts and formulas

There are no formulas in this topic. These are the facts to learn; nothing here is given in the exam.

Fact	Status
Brute force: trial and error, repeated combinations until the password is found, often by software	Learn it
Data interception: packets captured in transit (packet sniffer) and analysed by a third party	Learn it
DDoS: malware → bots → botnet → attack started → all bots request at once → server crashes	Learn it
Hacking: gaining unauthorised access to a computer system	Learn it
Virus (needs a host, runs when file run); worm (spreads itself over a network); Trojan horse (disguised as genuine software); spyware (records key presses, sends to third party); adware (unwanted adverts); ransomware (encrypts data, demands payment)	Learn it
Phishing: genuine-looking email → click link → fake website → details stolen	Learn it
Pharming: malicious code installed → real URL typed → redirected to fake website → details stolen	Learn it
Social engineering: manipulating people to give up data (phishing, baiting, shoulder surfing)	Learn it
Access levels: different permissions (none, read, edit, delete) per username	Learn it
Two-step verification: extra code sent to the user's registered device	Learn it
Firewall: criteria set, all traffic in and out checked, rejected if it fails; hardware or software	Learn it

Fact	Status
Proxy server: examines requests, limits rate, blocks IPs, caches pages, hides the server's IP address	Learn it
SSL: browser asks server to identify itself → digital certificate sent → browser authenticates it → encrypted connection; it newer version TLS	Learn

How to do it

In the Paper 1 questions we have tagged for this topic (42 questions, 2021–2025), the types came up this often. Parts of 2 of these (2021–2022) also asked about accidental data loss, which is no longer in the syllabus. 25 of the 42 questions mix more than one type, so the counts add up to more than 42.

Question type	Questions
Give (and explain) security solutions for a threat or situation	18
Describe how a threat works and/or its aim	15
Name or recognise threats and types of malware	11
Explain how a firewall or proxy server protects a system	11
Explain SSL/HTTPS and how to spot a secure website	10
Draw and annotate a diagram of a threat or firewall	6
Complete a term/definition table or a gap-fill paragraph	3

1. Give (and explain) security solutions for a threat or situation (18 questions)

1. **Identify the threat** in the stem and pick solutions that stop **that** threat. A solution that doesn't fit earns nothing.
2. **Give different solutions**, not the same one twice in other words, and not one the stem already gave.
3. If asked to **explain**, add **how** it helps **against this threat**, usually two linked points: what it does, and why that defeats the attacker.

The best matches:

Threat	Solutions
Brute force	Strong password; limit the number of attempts; two-step verification; biometrics
Hacking	Firewall; strong password; two-step verification; biometrics; access levels; automatic updates
Spyware capturing a login	Anti-spyware; biometrics; drop-down boxes or on-screen keyboard; asking for only some characters of the password
Phishing / pharming	Check the spelling and tone; check the sender's address; check the URL of the link; anti-malware scans of downloads; download only from trusted sources; never give personal details by email
DDoS	Proxy server; firewall; users scanning their computers with anti-malware (so they don't become bots)
Data interception	Encryption (SSL/HTTPS): intercepted data is meaningless without the key
Malware	Anti-malware; firewall; automatic updates
Social engineering	Staff training; privacy settings; access levels

Variations you will meet:

- **"Describe what is meant by access levels"**: different users get different permissions; some can only read data, some can change or delete it, some can't see it; linked to their username.

- **Solution plus a matched explanation** (1 + 2 marks each). For example: two-step verification (**1**); a code is sent to the user's registered device (**1**), which the hacker would also need to have (**1**).
- **A biometric password instead of a PIN**: it is a physical characteristic, unique to the user, can't be guessed or forgotten, and nothing is typed.
- **"Tick one other method"** to add to a username and password: two-step verification (a firewall or access levels don't make the login stronger).
- **Read the context**. A laptop that is never connected to a network doesn't need a firewall; "keep **stored** data safe" isn't answered by anti-spyware; "**software** methods" rules out a locked room.

2. Describe how a threat works and/or its aim (15 questions)

1. Write the **process** as a chain of steps, one per mark, in order, using the steps in "Understand it".
2. For the **aim**, say what the attacker **gets**: personal data, money, disruption, revenge, reputation damage.
3. For "**identify and describe**", name the threat (**1**), then two description points (**2**).

Variations you will meet:

- **Phishing** (up to 4 marks): genuine-looking email → user clicks the link → fake website → enters personal data → data used by a third party.
- **Pharming**: malicious code installed without the user knowing → redirects the real URL to a fake website → user enters details.
- **Brute force** (3 marks): trial and error; combinations entered repeatedly until the right password is found; can be done automatically by software.
- **Social engineering** (3 marks): manipulating or deceiving people (**1**), to get confidential data or make them make a mistake (**1**), plus an example (**1**).
- **Aims**. DDoS: disrupt a web server; revenge, reputation, ransom, testing. Phishing and pharming: obtain personal data. Brute force: steal, delete, change or lock data, damage reputation. **Don't repeat the aim the stem gives** ("to gain access to the account").
- **"Two ways the details could have been stolen"**: phishing, pharming, hacking, spyware, each with a description. If the stem says "one other", don't repeat the one given.

3. Name or recognise threats and types of malware (11 questions)

1. **Malware**: virus, worm, Trojan horse, spyware (keylogger), adware, ransomware. Three different malware can count as three threats.
2. **Not malware**: phishing, pharming (as a threat), hacking, DDoS, brute force, social engineering, data interception.
3. **Software that finds and removes malware**: anti-malware.

Variations you will meet:

- **"Tick the statement(s) that apply"** to each threat. Work from the key features: self-replicating = virus (and worm); records key presses = spyware; stops access to a website = DoS/DDoS; nothing is installed **on** the web server in a DoS.
- **"Pick the correct definition of spyware"**: it **records key presses and sends them to a third party**. The analysing of the data is done afterwards by the third party, not by the spyware.
- **Threats a proxy server protects against**: DDoS, hacking, malware, brute force (not phishing, which targets a person, not a server).
- **Identify and describe two malware** in a table: name each (**1**) plus its key features, as in the malware table above. Don't repeat one the question names.

4. Explain how a firewall or proxy server protects a system (11 questions)

1. **Firewall** (up to 5 marks): criteria are set (blacklist/whitelist of IP addresses, ports, applications); it examines traffic **coming in and going out**; compares it with the criteria; **rejects** traffic that doesn't meet them (and can warn the user); can **close ports** hackers use.
2. **Proxy server protecting a web server**: it is an **intermediary**; it examines each request; **limits or slows** the rate of requests; **blocks IP addresses** that send too many; **caches** common pages and answers those requests itself; **hides the server's IP address**.
3. Apply it to the stem: if the question is about hacking, say how the rules keep the hacker out; if it is about a DDoS, say how the requests are stopped before they **reach the web server**.

Variations you will meet:

- **"Tasks a proxy does that a firewall doesn't"**: hiding the (public) IP address; caching web pages.
- **Similarities and a difference**: both filter traffic, hold blacklists/whitelists, block unauthorised access, and can be hardware or software. A difference needs **both sides**: "a proxy hides the server's IP address, **whereas** a firewall does not". "A proxy has a cache" alone isn't enough.
- **"A firewall is software based"**: it can be **hardware or software**.
- **Gap-fills about a firewall** test the key words from the steps above: that it can be hardware or software, what it sits between, that criteria are set, that traffic is accepted or rejected, and which threats it helps stop. Try [0478/11/M/J/21 Q3](#).

5. Explain SSL/HTTPS and how to spot a secure website (10 questions)

1. **"Explain how a secure connection is created"** (up to 6 marks): browser asks the web server to identify itself; server sends its **digital certificate**; browser **authenticates** it; if valid, an **encrypted** connection is made (asymmetric) and data sent is meaningless if intercepted; if not valid, the connection is rejected and the user is told.
2. **Get the direction right**: the **browser asks**, the **server sends** the certificate, the **browser checks** it.
3. **"How does SSL secure the data?"**: it **encrypts** it, so intercepted data can't be understood; it uses digital certificates. "It makes a secure connection" repeats the name and earns nothing.

Variations you will meet:

- **"Two ways a user can check a site uses SSL"**: the URL starts `https`; a **padlock** is shown; view the **digital certificate**.
- **"Name the updated version"**: TLS. **"An alternative protocol"**: HTTPS or TLS.
- **Gap-fill** of the steps with *web browser*, *web server* and *encrypted*.

6. Draw and annotate a diagram of a threat or firewall (6 questions)

1. **Boxes and arrows only**: examiners report that time spent on artwork earns nothing. Draw the devices as labelled boxes.
2. **One annotated step per mark**: count the marks and write at least that many short labels on the arrows.
3. Use the diagrams in "Understand it":
 - **DDoS** (5–6 marks): third party sends malware; computers become bots; botnet; attack started; all bots send requests at once to the web server; server crashes / genuine users can't connect.
 - **Data interception** (4 marks): data sent from one device to another; examined in transit; packet sniffer; data sent to a third party and analysed.
 - **Firewall** (4 marks): traffic in both directions; criteria set; traffic compared with criteria; accepted or rejected.
 - **Pharming** (4 marks): user clicks a link or attachment; malicious code downloaded; user enters the real address; redirected to a fake website.

7. Complete a term/definition table or a gap-fill paragraph (3 questions)

1. Decide for each row whether you give the **term** or the **description**.

2. **Terms** must be exact: *proxy server, firewall, hacking, malware, bot, botnet, web server*.
3. **Descriptions** say what it **is** and what it **does**: hacking is "gaining unauthorised access to a computer system"; a firewall "filters traffic coming into and going out of a network, and can be hardware or software".

For a **gap-fill describing a process** (such as a DDoS), follow the process steps in "Understand it" in order: each blank is the next step's key word. Each word is used once, and the list always includes spare words that sound related but don't fit, so check each choice against the step. Try **0478/13/M/J/23 Q8**.

Worked examples

The bold codes show where marks are earned, as in Cambridge mark schemes. The number is how many marks.

- **B1** mark for a correct result on its own, with no method needed.
-

Example 1

A college IT technician keeps a log of problems reported by students.

(a) For each report, identify the type of malware most likely to be responsible. **[5]**

Report

A: "I installed a free video converter from a pop-up. It works fine, but my antivirus now finds several other programs I never installed."

B: "All my coursework files have strange file extensions and won't open. A message says I must pay to get them back."

C: "Three computers in the library became infected overnight, although nobody used them or opened any files."

D: "Adverts for games keep popping up on my screen, even when my browser is closed."

E: "Someone logged into my email the day after I used a library computer, and I'm sure no one saw my password."

(b) One student says report E was caused by phishing. Explain why this is unlikely. **[2]**

(c) The college sets anti-malware updates to install automatically. Explain why this helps keep the college's data safe. **[2]**

(a)

- A: **Trojan horse**: it was disguised as useful software and installed other malware hidden in it. **B1**
- B: **Ransomware**: the files have been encrypted and payment is demanded for the key. **B1**
- C: **Worm**: it spread across the network by itself, with no user opening a file. **B1**
- D: **Adware**: it displays unwanted adverts. **B1**
- E: **Spyware** (a keylogger): it recorded the key presses as the password was typed and sent them to a third party. **B1**

(b) Phishing needs the user to receive an email and click a link to a fake website, where they type their details. **B1** Here the student only typed the password on a library computer, with no email or fake site involved, so software on that computer recording key presses is more likely. **B1**

(c) New malware appears all the time; each update adds it to the list the anti-malware checks files against, so newer malware can be detected and removed. **B1** Automatic updates are installed as soon as they are released, without relying on staff or students to remember. **B1**

Example 2

A delivery app sends customers' names, addresses and card numbers to the company's web server. Many customers use the app on free public Wi-Fi in cafés.

(a) Explain how a criminal in the café could obtain customers' card numbers without hacking the customers' phones or the company's server. [3]

(b) The company's web server uses SSL. One morning its digital certificate has expired. Describe what happens when a customer's browser connects to the server that morning, and explain why this protects the customer. [4]

(a) Any three:

- the card numbers are sent across the network as data packets **B1**;
- the criminal captures the packets while they are in transit over the Wi-Fi, for example with a packet sniffer **B1**;
- the captured data is examined / analysed to find the card numbers **B1**;
- this works without accessing either device, because the data is taken on its way between them.

(b) Any four:

- the customer's browser asks the web server to identify itself **B1**;
- the web server sends its digital certificate to the browser **B1**;
- the browser checks the certificate and finds it is not valid **B1**;
- so no secure (encrypted) connection is made: the connection is rejected and the customer is warned **B1**;
- this protects the customer because the server can't be proved genuine, so they are not led into sending card details to a site that may be fake, or unencrypted.

Example 3

A festival sells tickets on its website. The web server can handle 3000 requests per second; on a busy day it normally receives about 1200. When tickets go on sale, the server crashes. The log shows requests from 25 000 different home computers, each sending 4 requests per second.

(a) Calculate how many times more requests per second the server received than it can handle, and explain why this points to a DDoS attack rather than keen customers. [3]

(b) Describe how the attacker could have got control of 25 000 home computers. [3]

(c) The festival puts a proxy server in front of the web server, with a rule to block any IP address that sends more than 10 requests in 5 seconds. Explain what the proxy server does with each incoming request under this rule, and what happens to a bot's requests and to those of a genuine customer who sends 3 requests in 5 seconds. [4]

(a) $25\,000 \times 4 = 100\,000$ requests per second, and $100\,000 \div 3000 \approx 33$, so about 33 times what the server can handle. **B1** The requests come from a huge number of different computers at once, each sending requests continuously at the same rate **B1**, which fits bots in a botnet being told to attack together, not people buying tickets. **B1**

(b) Any three:

- the attacker spread malware, for example in an email attachment or a download **B1**;
- users installed it without knowing, and it turned each computer into a bot **B1**;
- the infected computers together form a botnet, which the attacker controls **B1**;
- the attacker then told every bot to send requests at the same time.

(c) Any four:

- the proxy is an intermediary: requests go to it, not straight to the web server **B1**;
- it examines each request and counts the requests from each IP address **B1**;
- each bot sends $4 \times 5 = 20$ requests in 5 seconds, more than 10, so its IP address is blocked and its requests never reach the web server **B1**;
- the genuine customer sends only 3, under the limit, so their requests are passed on **B1**;

- it can also answer common requests from its cache and hide the web server's IP address, so less traffic reaches the server and the attacker can't target it directly.

Example 4

A small dental practice keeps patient records on its network. Last month the receptionist received a phone call from someone claiming to be from the practice's IT company, who asked for her password "to fix a fault". She gave it.

- (a) Name this threat and describe what is meant by it. **[3]**
- (b) The practice already has a firewall and anti-malware. Explain why they did not prevent this. **[2]**
- (c) Explain how access levels would reduce the harm done by the caller using the receptionist's password. **[3]**
- (d) Staff often post about work on social media. Explain how privacy settings help protect the practice. **[2]**
- (a)** Social engineering. **B1** The attacker manipulates or deceives a person, here by pretending to be a trusted IT worker **B1**, so that they hand over confidential data such as a password. **B1**
- (b)** A firewall and anti-malware protect against traffic and malicious software. **B1** Here nothing malicious passed through the system: a person gave the password away, and the caller logs in with the correct password, like a genuine user. **B1**
- (c)** Any three:
- each user is given permissions linked to their username **B1**;
 - the receptionist only needs appointments and contact details, so her account can't open treatment records **B1**;
 - she may be able to read some data but not edit or delete it **B1**;
 - so the caller can only see or change the small amount of data her account allows.
- (d)** Privacy settings let staff choose who can see their posts and profile, for example only friends. **B1** This limits the personal and work details an attacker can find to make a convincing call, or to guess passwords and security answers. **B1**

Common mistakes

- **Mixing up phishing and pharming**, giving each the other's description. Phishing starts with an **email** and a **link**; pharming starts with **malicious code** that **redirects** a real URL.
- **"The user opens the email and is taken to a fake website."** Opening an email does nothing: the user has to **click a link or attachment**. Several examiner reports mention this.
- **Calling phishing or hacking malware**. Malware is software installed on a computer; phishing is a trick email and hacking is gaining unauthorised access.
- **Vague brute-force answers**. "Guessing the password" gets one mark at most. Describe **trial and error**, trying **combinations repeatedly until one works**, often **automatically by software**.
- **Saying a DoS is installed on the web server**. The malware is on the **bots**; the server is only the target of their requests.
- **Answering a different question**. Asked how a DDoS is **prevented**, many students describe how it is **carried out**. Asked how an SSL connection is **created**, many describe what encryption is. Answer the question asked.
- **Reversing the SSL steps**: the **browser** asks the **server** to identify itself, and the **server** sends the certificate. It is the web server, not the website, that holds the certificate.
- **"Anti-hacking software"**. There is no such thing: say **firewall** or **proxy server**.
- **Giving a threat that doesn't fit**. Phishing can't be done to a web server; a virus isn't used to steal personal data by email. Check the threat matches the situation.
- **Social engineering and access levels**. Examiners say very few students can describe either. Learn them: "manipulating people to obtain data, for example ..."; "different users have different permissions to read, edit or delete data".
- **One-sided differences**. "A proxy hides the IP address" is only half a difference; add "whereas a firewall does not".
- **Artwork in diagrams**. Marks are for the annotated steps, not drawings of computers.

- **Repeating the stem.** If the question says the aim is to gain access, or names one malware, give something **else**.

How to get the marks

- **"State", "identify", "give"** (1 mark each): the exact term: *spyware*, *proxy server*, *two-step verification*, *TLS*. For a tick question, tick exactly one box unless told otherwise.
- **"Describe" a threat**: one step per mark, in the order it happens. **"Describe the aim"**: what the attacker gains.
- **"Explain" a solution**: the solution, then **how** it helps against **this** threat: "Limiting login attempts (**1**) means the account locks after a few wrong passwords (**1**), so software can't keep guessing (**1**)."
- **"Explain the difference"**: matched pairs joined by "whereas".
- **"Draw and annotate"**: simple boxes, arrows, one short label per step, at least as many labels as marks.
- **Use the context.** If the scenario is a web server, choose threats and solutions that affect a web server; if the laptop is never online, a firewall adds nothing; don't repeat what the stem gives.
- **Different answers must be different.** "Anti-virus" and "anti-malware" given as two solutions may only earn one mark; "strong password" and "long password" are the same point.

Quick check

1. A student writes: "Phishing is a type of virus that steals your bank details." Give two reasons why this statement is wrong.
2. An email says it is from your school and contains a link displayed as `www.hilltopacademy.edu`. When you hover over it, the address shown is `http://hilltop-academy-login.net/verify`. Give two signs in this address that the link is not genuine, and one other thing in the email you should check.
3. State one difference between how a virus and a worm spread.
4. A phone locks for one hour after every 5 wrong PIN attempts. Its PIN has 4 digits. In the worst case, about how many hours would a thief need to try every possible PIN by hand? Explain what this shows about limiting attempts.
5. A school keeps exam marks on its network. Explain why teachers are given edit access to the marks while students are given read-only access to their own marks.

Answers

1. Phishing is not malware (not a virus): it is a trick email or message, and nothing needs to be installed. It works by getting the user to click a link to a fake website and type in their details themselves; a virus is code that copies itself into other files and damages data.
2. Signs: the domain is different from the school's real one (`hilltop-academy-login.net`, with extra words and a different ending), and it uses `http`, not `https`. Also check the sender's email address, and the spelling and tone of the email (for example an urgent threat or a generic greeting).
3. A virus needs a host file and only spreads when that file is run (by a user); a worm copies itself across a network by itself, with no host and no user action.
4. There are $10^4 = 10\,000$ possible PINs, which is $10\,000 \div 5 = 2000$ batches of 5 attempts. There is a one-hour lock after every batch except the last, so 1999 hours, about 83 days. Limiting attempts makes a brute-force attack far too slow to be practical.
5. Access levels give each user only the permissions they need. Teachers need to enter and correct marks, so they can edit; students only need to see their own marks, so they can read them but can't change them (or see other students' marks). If a student's account were misused, the marks could not be altered.

Past questions to try

- [0478/12/M/J/23 Q7](#): draw and annotate a DDoS, its aims and two solutions.
- [0478/12/O/N/23 Q8](#): a data interception diagram and a solution.
- [0478/11/M/J/23 Q8](#): how a brute-force attack works, its aims, malware and solutions.
- [0478/12/O/N/22 Q6](#): checking for SSL, a proxy server, and stopping spyware at login.