

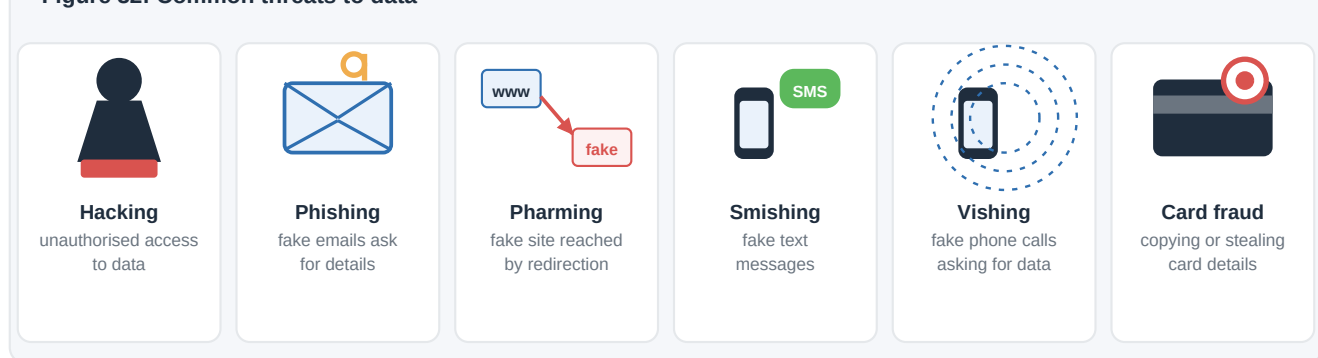
8.3.1 Threats to Data

Syllabus 2026 - 2028

WHAT YOU NEED TO KNOW

- Characteristics and effects of threats to data: hacking, phishing, pharming, smishing, vishing, viruses, malware and card fraud
- Measures to protect data from hacking
- Methods to help prevent phishing, pharming, smishing and vishing
- Preventative action to avoid infection from a downloaded file
- Card fraud: shoulder surfing, card cloning and key logging

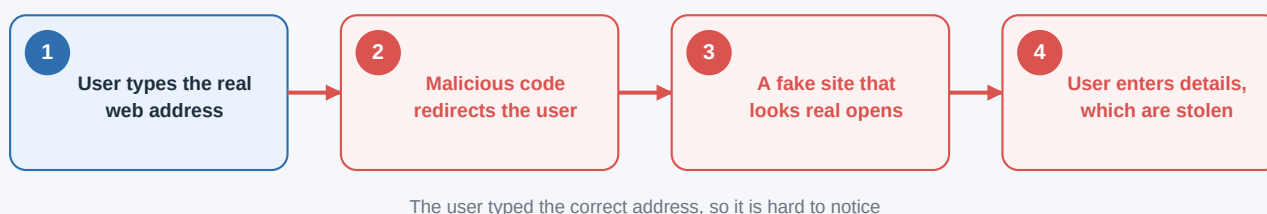
Figure 32: Common threats to data



Threat	What it is	Effect	Prevention
Hacking	Gaining unauthorised access to a computer or network, for example by guessing passwords or using weaknesses in software.	Data is stolen, changed or deleted; identity theft; fraud; damage to systems	Use a firewall; strong passwords that are changed regularly; two-factor authentication; keep software updated; anti-malware; encryption; user access levels
Phishing	Fake emails, pretending to be from a bank or other trusted source, that ask the user to click a link or give personal data.	Passwords and card details are stolen; money is lost; identity theft	Do not click links or open attachments in unexpected emails; check the sender and for spelling mistakes; type web addresses yourself; use spam filters; report the email
Pharming	Malicious code on a computer or server redirects users to a fake website that looks real, even when they type the correct address.	Login and card details are stolen without the user realising	Use anti-malware and anti-spyware; keep software updated; check the address and padlock (https); use a firewall; do not enter details on a site that looks odd
Smishing	Phishing by SMS text message, with a link or a number to call.	Malware is installed or details are stolen	Do not click links or reply to unknown messages; do not call numbers in messages; contact the organisation using its official number; block and report the sender
Vishing	Phishing by telephone call or voicemail, where a caller pretends to be from a bank or support and asks for details or codes.	PINs, passwords and codes are given away; money is stolen	Never give PINs or passwords by phone; hang up and call the official number; be wary of callers who rush you; do not trust the caller ID

Threat	What it is	Effect	Prevention
Viruses and malware	A virus is a program that copies itself and spreads; malware is any harmful software, including worms, trojans, spyware and ransomware.	Files are corrupted or deleted; the computer slows down; data is stolen; files are locked for a ransom	Scan every downloaded file with anti-malware; download only from trusted sources; do not open unexpected attachments; keep software updated; do not use pirated software; use a firewall
Card fraud	Stealing card details to make payments. Methods are shoulder surfing (watching a PIN being entered), card cloning (copying the data from a card using a skimmer on an ATM or reader) and key logging (spyware that records key presses).	Money is stolen; identity theft; the victim's account is affected	Cover the keypad when entering a PIN; use chip and PIN or contactless; check ATMs for tampering; keep the card in sight; use anti-spyware; check statements regularly; report loss at once

Figure 33: How pharming steals data



Avoiding infection from a downloaded file

- Only download from **trusted websites** and official stores
- **Scan** the file with up-to-date anti-malware before opening or installing it
- Do not open attachments or follow links from **unknown** senders
- Keep the operating system and software **updated** and use a firewall
- Do not run files with strange names or types, such as a program sent as a picture

EXAM TIP

Know how to **separate** the four similar threats: **phishing** uses email, **smishing** uses text messages, **vishing** uses phone calls and **pharming** uses a redirect to a fake website. For each one, give a way to prevent it.

Key terms

Term	Meaning
Hacking	Unauthorised access to a computer or network.
Phishing	Fake emails that trick users into giving data.
Pharming	Redirecting users to a fake website.
Smishing	Phishing by SMS text message.
Vishing	Phishing by phone call.
Malware	Software designed to harm or steal data.
Shoulder surfing	Watching someone enter a PIN or password.
Card cloning	Copying card data onto another card.
Key logging	Recording key presses with spyware.
Skimmer	A device that copies card data.

Practice questions

Answer each question in full sentences. Command words used: State (give a short answer), Describe (say what it is like), Explain (give reasons), Analyse (break it down and examine it), Suggest (apply your knowledge to a situation), Compare and contrast (similarities and differences), Evaluate (weigh up and reach a judgement).

No.	Question	Marks
1	State the meaning of pharming.	[2]
2	State two examples of card fraud.	[2]
3	Describe how phishing could be used to steal a user's password.	[3]
4	Explain how smishing is different from vishing.	[2]
5	Analyse how a key logger could lead to card fraud.	[3]
6	Suggest three ways of avoiding infecting a computer with malware from a downloaded file.	[3]
7	Compare and contrast phishing and pharming.	[4]
8	Evaluate the measures that can be taken to protect data from hackers.	[6]

Total: 25 marks