Common Attacks — Phishing and Malware

Phishing tricks people, malware tricks computers — learn how both attacks work and how to stop them.

Introduction

Most attacks do not break through a wall. They walk through the front door — because someone opened it for them. **Phishing** is a message that pretends to be from someone you trust, and tricks you into giving away a password, a code, or money. **Malware** is software built to harm: it steals, spies, locks your files, or takes over your computer.

Phishing attacks people. Malware attacks computers. But they usually work together: the phishing message is the delivery, and the malware is the payload. "Your parcel is waiting — click here to track it" — the link downloads malware, and the malware steals your passwords.

In this lesson you will learn to spot a phishing message in seconds, meet the main kinds of malware, and build the habits that stop both.

(Roman Urdu: Phishing ka matlab hai dhoka — aisa message jo bank ya dost jaisa lage, magar password ya paisa chura le. Malware bura software hai jo computer ko nuksan pahunchata hai. Aksar dono aik saath aate hain: phishing link, malware download.)

The key insight: phishing works because it uses urgency and trust, not technology. A message that makes you panic — "your account will close in 1 hour!" — is trying to switch off your thinking. Slowing down is the defence.

Key points

- **Phishing is a fake message that pretends to be from someone trusted.** Email, SMS (smishing), phone calls (vishing), and fake websites all count.
- **Phishing always wants one of three things: your password, your money, or a click that installs malware.** If a message asks for any of these, slow down.
- **Signs of phishing: urgency ("act now!"), a sender address that is almost right (support@amaz0n.com), bad grammar, a link that goes somewhere different from what it shows, and an unexpected attachment.**
- **Spear phishing targets one person with personal details.** "Hi Ali, here is your university fee receipt" — with your real name and university. Harder to spot, so verify through a second channel.
- **Malware is short for malicious software.** Main kinds: virus (spreads by attaching to files), worm (spreads by itself across networks), trojan (pretends to be useful software), ransomware (locks your files and demands money), spyware (watches you quietly), adware (floods you with ads).
- **Ransomware's defence is backups.** If your files are backed up somewhere safe, a locked computer is an annoyance, not a disaster — and you never pay the ransom.

- **Antivirus helps, but it is the last line, not the first.** The first line is you: don't click, don't download, don't trust the unexpected message.
- **Verify through a second channel.** A message says "bank calling"? Hang up and call the bank's official number yourself. A link says "parcel tracking"? Open the courier's app yourself.

Examples

Example 1 — Spot the phish (read this email)

```
From:    security@micros0ft-support.com
Subject: URGENT: Your account will be closed in 1 hour!
Body:    Dear Customer, we found unusual activity. Click here
         immediately to verify your account or lose access.
         [VERIFY NOW]
```

Five red flags: (1) "micros0ft" with a zero, not Microsoft's real domain; (2) "URGENT ... 1 hour" — manufactured panic; (3) "Dear Customer" — a real company uses your name; (4) a link asking you to "verify" — real companies rarely do this by email; (5) a threat (lose access). One flag is enough to stop and verify another way.

Example 2 — The same attack, three channels

```
Email:    "Your parcel is held at customs. Pay Rs 500 to release it."
SMS:      "Your bank account is blocked. Click this link to unblock."
Call:     "This is your bank. Share the code we just sent you."
```

Same trick, three doors. The defence is the same every time: do not use the link or number in the message — open the real app, or call the real official number, yourself.

Example 3 — Meet the malware family

```
Virus:     attaches to a file; spreads when you share the file.
Worm:      spreads alone across a network; no click needed.
Trojan:    looks like a free game or a "cracked" app; opens a
           back door once you install it.
Ransomware: encrypts your photos and notes; shows a payment demand.
Spyware:   records what you type; sends passwords to the attacker.
Adware:    floods your screen with ads; often comes with free apps.
```

A trojan is the most common delivery for students: a "free" version of a paid app that costs you your passwords instead.

Example 4 — Ransomware: why backups win

```
Without backup:
  files locked -> pay the criminal (and maybe still lose them)
  -> or lose years of photos and notes forever.

With backup:
  files locked -> wipe the computer, restore from backup
  -> lose at most one day of work. No payment, no panic.
```

Backups turn ransomware from a disaster into a bad afternoon. Keep one copy somewhere the ransomware cannot reach — for example, a drive you unplug after backing up, or cloud storage with version history.

Quick recap

- Phishing pretends to be trusted and wants your password, money, or a click.
- Red flags: urgency, almost-right sender, generic greeting, mismatched link, unexpected attachment.
- Spear phishing targets one person with real personal details — verify through a second channel.
- Malware family: virus, worm, trojan, ransomware, spyware, adware.
- Backups beat ransomware; slowing down beats phishing.

Common mistakes

1. **Clicking before thinking** — urgency is the weapon; panic is the goal. Fix: stop, breathe, verify another way.
2. **Trusting the display name** — "Bank Support" can be written by anyone; the real address behind it is what matters. Fix: check the actual sender address and the real link destination (hover, don't click).
3. **Downloading "free" cracked apps** — the most common trojan delivery for students. Fix: if software is paid, the free copy is usually the trap.
4. **Paying a ransom** — payment funds more crime and often does not return your files. Fix: restore from backup; report the attack.
5. **Thinking antivirus makes you safe** — new malware appears daily, and antivirus cannot recognise what it has never seen. Fix: antivirus plus careful habits, not antivirus instead of them.

Practice

1. Find one phishing-style message in your own inbox or spam folder. List every red flag in it — sender, urgency, greeting, link.
2. Write the three things phishing always wants (password, money, a click) on a sticky note. Next time a message asks for one, you will recognise the pattern.

3. Check your backup today: if your phone was stolen right now, which photos and notes would survive? Write the answer in one line.
4. Practise the second-channel rule: a message claims to be from your bank. Write the exact steps you would take to check it without using anything in the message.
5. Explain the difference between a virus, a worm, and a trojan to a friend, using one real-life comparison for each.

Practice quiz

1. What does a phishing message usually want?

- Your password, your money, or a click that installs malware
- Your opinion on a product
- A software update
- Your phone number for a prize draw

Answer: Your password, your money, or a click that installs malware

2. Which of these is a red flag for phishing?

- The email uses your real name
- Urgency — 'act in 1 hour or lose access' — plus a sender address that is almost right
- The email has no attachments
- The email arrived in the morning

Answer: Urgency — 'act in 1 hour or lose access' — plus a sender address that is almost right

3. What is ransomware, and what beats it?

- Software that shows ads; an ad-blocker beats it
- Software that locks your files and demands money; backups beat it
- Software that spies on typing; a new keyboard beats it
- Software that deletes files; antivirus always beats it

Answer: Software that locks your files and demands money; backups beat it

---

Watch the Code Scope channel: https://www.youtube.com/@CodeScopePK — this lesson's own video joins the channel when it is recorded.

Read online: https://scopetreasure.com/notes/cs-phishing-malware · More free tools and notes at https://scopetreasure.com