Social Engineering Awareness Course

Essential knowledge for everyone in today's digital world

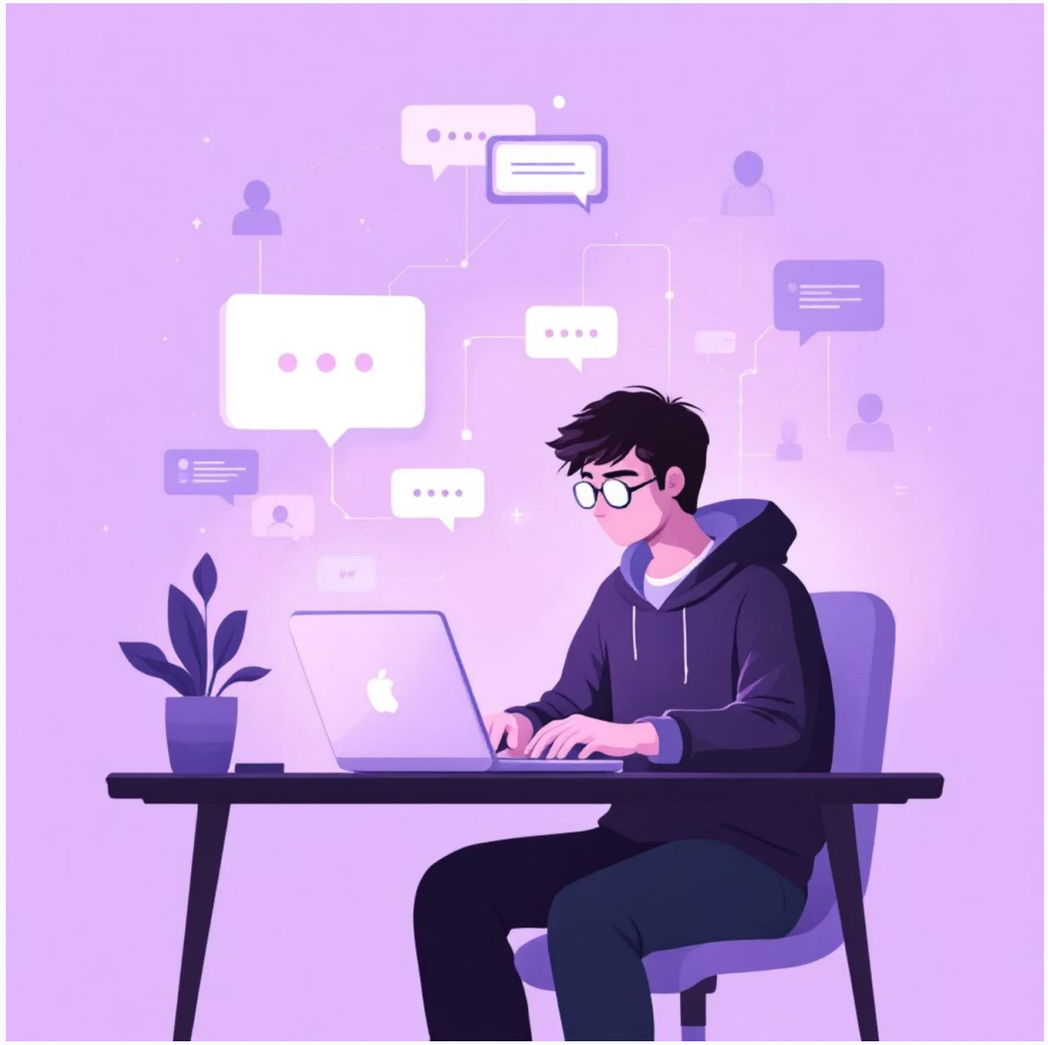
GENERAL PUBLIC

CHAPTER 1

What is Social Engineering?

Social engineering is the art of manipulating individuals into exposing confidential information, performing actions, or providing access to secure systems by exploiting human psychology rather than technical vulnerabilities.

Cybercriminals exploit trust, emotions, and authority to deceive people. These attacks often bypass traditional security measures like firewalls and antivirus software, making human awareness the critical defense.



Individuals

Personal accounts, financial data, identity theft

Organizations

Corporate secrets, customer data, intellectual property

Government

Classified information, national security, infrastructure

⚠ ATTACK TYPES

Common Social Engineering Attacks

Phishing

Fraudulent emails pretending to be from trusted sources like banks, retailers, or colleagues, often containing malicious links or attachments designed to steal credentials.

Example: An email claiming to be from your bank asking you to verify account details. The link leads to a fake website designed to harvest your login information.

Smishing & Vishing

SMS text messages (smishing) and voice phone calls (vishing) that create urgency or fear to manipulate victims into divulging sensitive information or making immediate payments.

Example: A scammer posing as an IRS agent demands immediate payment over the phone, threatening arrest or legal consequences if you don't comply.

Spear Phishing & Whaling

Highly personalized, targeted email attacks aimed at specific individuals or high-level executives, using researched personal details to appear legitimate and trustworthy.

Example: A fake email appearing to be from your company CEO instructs you to urgently transfer funds to an offshore account for a confidential business deal.

More Attack Vectors to Watch For

Baiting & Pretexting

Deception-based scams using fake promises, free offers, or fabricated scenarios to trick victims into downloading malware or revealing confidential information.

- Free music or software downloads containing malware
- USB drives labeled "Confidential" left in public spaces
- Fake job offers requesting personal information

Tailgating/Piggybacking

A physical security breach where attackers gain unauthorized access to restricted facilities by following authorized personnel through secure entry points.

- Impersonating delivery drivers or maintenance workers
- Asking employees to "hold the door"
- Once inside: stealing devices, accessing files, installing malware

PSYCHOLOGY

How Attackers Manipulate Your Mind

Social engineers exploit fundamental human emotions and cognitive biases to bypass our rational thinking. Understanding these tactics is your first line of defense.

Creating Urgency

Scammers manufacture artificial time pressure and fear to force quick decisions without critical thinking.

> "Your account will be locked in 24 hours if you don't verify now!"

Exploiting Trust

Impersonating authority figures like CEOs, IT support, government officials, or trusted brands to gain instant credibility.

> "This is your bank's fraud department. We need your PIN to secure your account."

Guilt & Fear

Playing on deep emotions to cloud judgment and override normal security awareness through emotional manipulation.

> "Your grandson is in jail and needs bail money immediately—don't tell anyone!"

CHAPTER 2

Insider Threats: The Enemy Within

What Are Insider Threats?

Security risks posed by individuals who have legitimate access to organizational systems—employees, contractors, business partners, or vendors. These threats can be accidental or intentional.

01

Negligent Employees

Well-meaning staff who accidentally compromise security by clicking phishing links, mishandling sensitive data, or using weak passwords.

02

Malicious Insiders

Disgruntled or financially motivated employees who intentionally steal company secrets, sabotage systems, or sell confidential information.

03

Planted Moles

Outside attackers who infiltrate organizations by posing as legitimate employees, contractors, or partners to gain access from within.

Recognizing Insider Threat Warning Signs

Suspicious Data Access

Employees accessing sensitive files, databases, or systems that are completely unrelated to their job responsibilities or role requirements.

Unusual Working Hours

Logging into systems at odd times—late nights, weekends, holidays—especially when there's no legitimate business reason for doing so.

Security Policy Violations

Repeatedly attempting to bypass security controls, disable monitoring tools, or circumvent established protocols and procedures.

Real-World Examples

The Departing Employee

An employee downloads gigabytes of proprietary company documents, customer lists, and trade secrets onto a personal USB drive just days before submitting their resignation.

The Protocol Breaker

A staff member repeatedly tries to disable security cameras, share their access badge with others, or access restricted server rooms without authorization.

The Impersonator

An unknown person wearing a fake employee badge and carrying forged credentials gains entry to secure areas by following authorized personnel through security checkpoints.

CHAPTER 3

Common Fraud & Scam Tactics

Scammers constantly evolve their techniques, but understanding common patterns helps you stay protected. Here are the most prevalent fraud schemes targeting individuals today.

Online Shopping Fraud

Fake e-commerce websites that look legitimate but steal your credit card information and personal details without delivering any products. Often advertised through social media ads.

Government Impersonation

Scammers posing as IRS agents, FBI officials, or Social Security Administration representatives demanding immediate payment for fake taxes, fines, or penalties.

Romance Scams

Fraudsters create fake online dating profiles, build emotional relationships over weeks or months, then exploit victims financially with fabricated emergencies or investment schemes.

Tech Support Scams

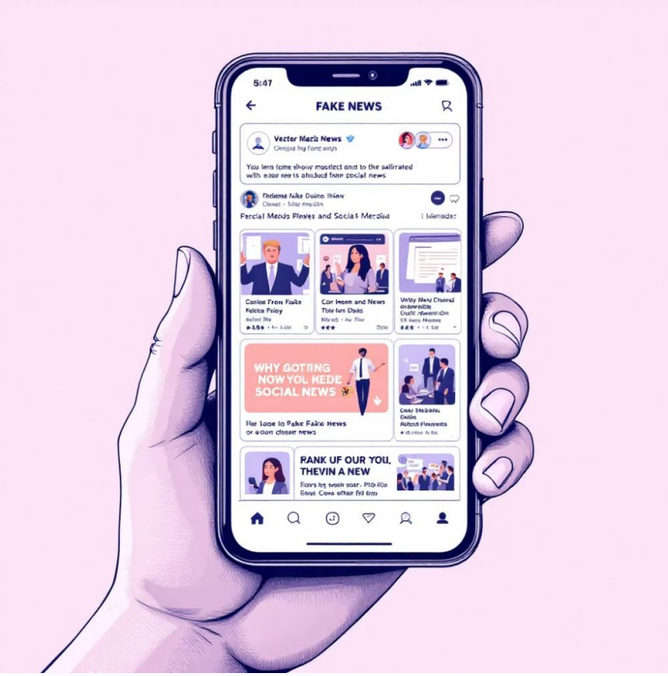
Fake IT helpdesks contact victims claiming their computer is infected with viruses, then trick them into installing remote access malware or paying for unnecessary "repairs."

Real Example: A scammer calls claiming to be from Microsoft, convinces the victim their computer has critical errors, charges $300 for fake repairs, and installs spyware to steal banking credentials.

Influence Campaigns & Digital Misinformation

The Misinformation Threat

Organized efforts to manipulate public opinion, spread false narratives, and influence decision-making through social media platforms, fake news sites, and coordinated bot networks.



Fake Profiles & Bot Networks

Automated accounts and fabricated personas that spread misleading content, amplify false narratives, and create artificial consensus on social platforms.

Deepfake Technology

AI-generated videos and audio recordings that convincingly impersonate public figures, celebrities, or company executives to spread false statements.

Fake Reviews & Testimonials

Fabricated product reviews, business ratings, and customer testimonials designed to influence purchasing decisions or damage competitor reputations.

Verify the Source

Check if the information comes from a credible, established news organization or verified account.

Cross-Reference

Look for the same story on multiple reputable news outlets before believing or sharing.

Use Fact-Checkers

Leverage tools like Snopes, FactCheck.org, or PolitiFact to verify suspicious claims.

Example: A viral social media post falsely claims a famous celebrity endorsed a cryptocurrency investment scheme. The deepfake video looks real, but fact-checking reveals the celebrity never made such statements.

YOUR DEFENSE

Defensive Strategies Against Social Engineering

Protection starts with awareness and healthy skepticism. Here are essential practices to safeguard yourself and your organization from social engineering attacks.

1 Be Skeptical

Always verify unexpected requests for information, money, or access—even if they appear to come from trusted sources. When in doubt, contact the organization directly using official contact information.

2 Inspect Links

Hover over links before clicking to reveal the actual destination URL. Look for misspellings, unusual domains, or mismatched addresses that indicate phishing attempts.

3 Protect Personal Info

Legitimate banks, government agencies, and reputable companies never ask for passwords, PINs, Social Security numbers, or other sensitive details via email, text, or phone.

4 Trust Your Instincts

If something feels wrong, suspicious, or too good to be true, it probably is. Take time to think critically before responding to urgent requests or unexpected opportunities.

Remember: You are the strongest defense

Technology alone cannot protect against social engineering. Your awareness, critical thinking, and cautious behavior are the most effective security measures available.

Final Example: You receive an email from "Amazon Support" with your name and recent order details, asking you to reset your password using a provided link. The email looks legitimate, but hovering over the link reveals a suspicious domain. You delete the email and log into Amazon directly through your browser—no password reset was needed. You just prevented a credential theft attack.

CHAPTER 4: DIGITAL IDENTITY

How to Secure Your Digital Identity

In an increasingly interconnected world, protecting your digital identity is paramount. This involves a combination of smart habits and security tools to safeguard your personal information and online presence.

Strong Passwords & Biometrics

Create unique, complex passwords for each account. Use a password manager to keep track of them and enable biometric authentication (fingerprint, facial recognition) when available for an extra layer of security.

Enable Multi-Factor Authentication (MFA)

Always activate MFA on your accounts. This requires a second form of verification (like a code from your phone) in addition to your password, significantly reducing the risk of unauthorized access.

Regularly Monitor Accounts

Periodically check your bank statements, credit reports, and online account activity for any suspicious transactions or unauthorized logins. Early detection is key to mitigating damage.

Avoid Oversharing Personal Information

Be cautious about what you share on social media and other online platforms. Limit personal details that could be used by social engineers to craft targeted attacks against you.

Example: You receive a notification that someone tried to log into your email from an unknown device. Because you have MFA enabled, the attempt was blocked, and you immediately changed your password and reviewed recent activity, preventing a potential takeover.

WORKPLACE SECURITY AWARENESS

Workplace Security Awareness

Cultivating a strong security posture in the workplace is a shared responsibility. Understanding common threats and best practices is crucial for protecting sensitive company data and systems.

Email Safety & Phishing

Be vigilant with emails, especially those with suspicious links or attachments. Always verify the sender's identity and look for warning signs of phishing attempts before clicking or downloading anything.

Device Security Best Practices

Ensure all work devices are password-protected, kept updated with the latest software and security patches, and never left unattended. Use strong, unique passwords for each system.

Verifying Unexpected Requests

Treat any unexpected requests for sensitive information, access, or financial transfers with extreme caution. Always verify such requests through official, established channels, not by replying directly to the sender.

Example: An employee receives an urgent email from "the CEO" requesting an immediate wire transfer to a new vendor. The employee, trained in security awareness, recognizes this as a potential scam and verifies the request through a direct phone call to the CEO's known number, preventing a significant financial loss.

INCIDENT RESPONSE

Recognizing & Reporting Incidents

Prompt identification and reporting of security incidents are critical to minimizing damage and ensuring a swift, effective response. Knowing what to look for and the proper channels to report through can make all the difference.

Identify Warning Signs

Be aware of indicators like unusual system behavior, suspicious emails or messages, unexpected pop-ups, unauthorized network activity, or compromised accounts. Trust your instincts if something seems off.

Document the Incident

Record all relevant details, including screenshots, timestamps, affected systems, and any observed anomalies. This information is vital for investigation and analysis.

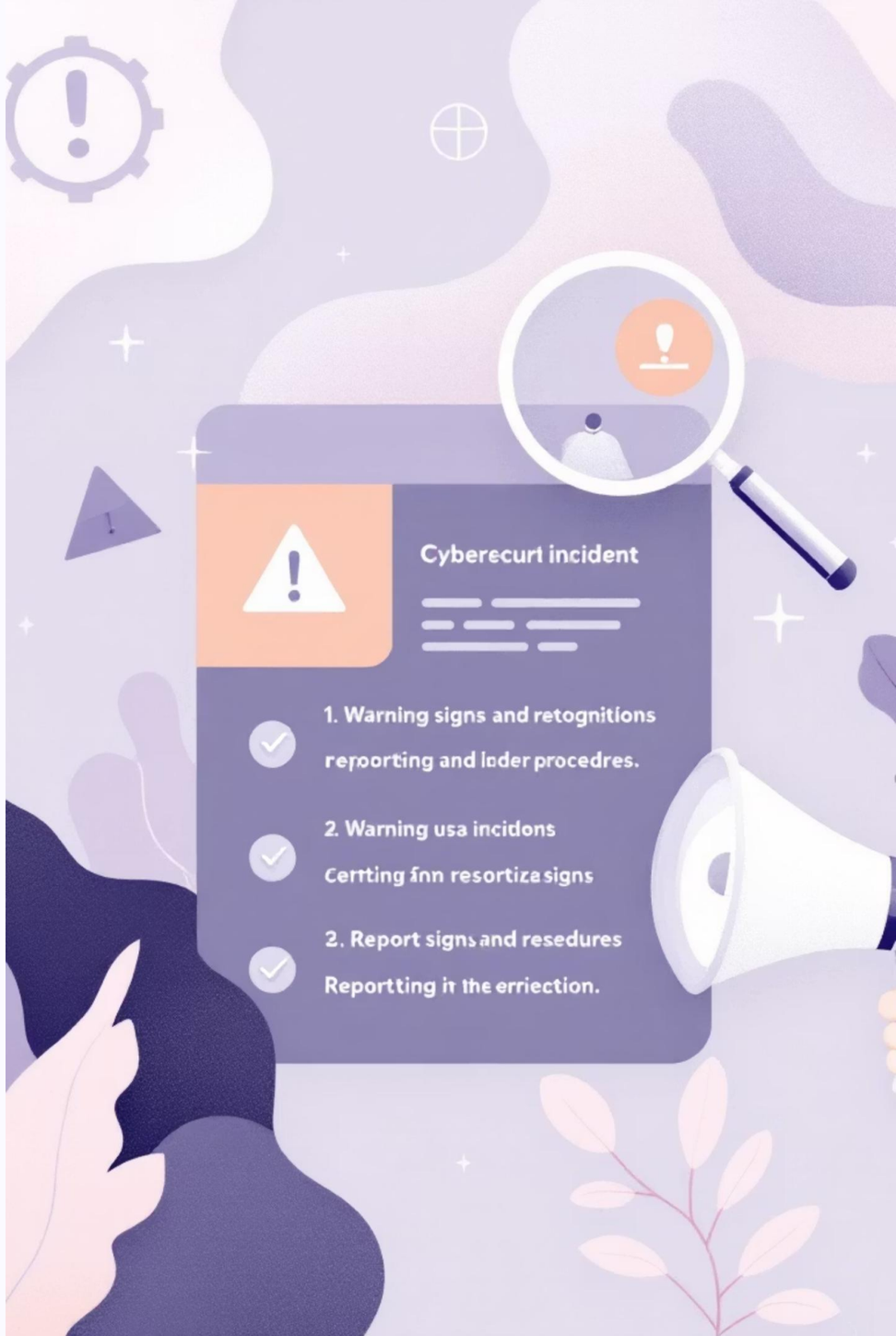
Report Immediately

Notify your organization's IT or security department through established channels. Do not try to resolve the issue yourself unless you are specifically authorized and trained to do so.

Cooperate with Response Team

Follow all instructions from the incident response team. Provide any requested information and be prepared to assist in the investigation and remediation efforts.

Example: You notice your computer acting unusually slow, and a new, unknown program keeps trying to access the internet. You immediately disconnect your device from the network, take screenshots, and report the issue to your IT help desk. Your quick action prevents a potential malware infection from spreading across the company network.



Social Engineering Awareness Quiz

QUESTION 1 OF 6

Which of the following is an example of baiting?

A

A fake tech support call demanding remote access

B

A pop-up ad offering free software that installs malware

C

An email asking you to confirm your bank details

D

A phone call pretending to be a government official

ANSWER — QUESTION 1

Which of the following is an example of baiting?

A ❌

A fake tech support call demanding remote access — **This is vishing, not baiting.**

B ✔

A pop-up offering free software that installs malware — **Baiting lures victims with enticing free offers.**

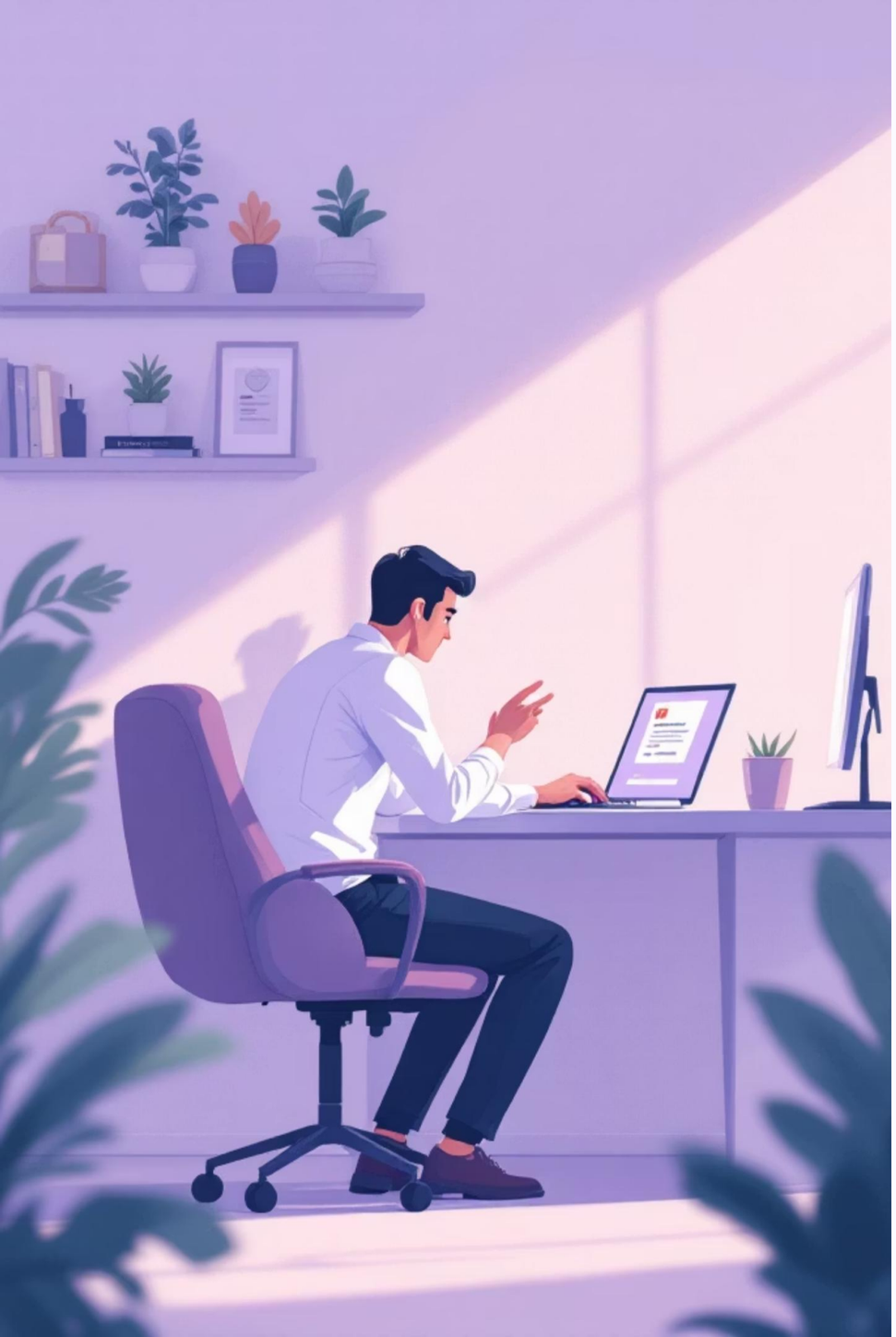
C ❌

An email asking you to confirm bank details — **This is phishing, not baiting.**

D ❌

A phone call pretending to be a government official — **This is pretexting, not baiting.**

Key Takeaway: Baiting uses attractive offers — like free downloads or USB drives — to trick users into triggering malware.



QUESTION 2 OF 6

Urgent Wire Transfer Request

You receive an urgent email from your boss asking for a wire transfer. What do you do?

A
Transfer the money quickly to avoid issues

B
Reply to the email and ask for confirmation

C
Call your boss using a known phone number to verify

D
Ignore the email completely

ANSWER — QUESTION 2

Urgent Wire Transfer Request

✔ Correct Answer: C

Call your boss using a known phone number to verify. **Direct verbal confirmation is the only reliable way to prevent fraud.** Scammers rely on urgency to bypass your judgment — slow down and verify first.

Why the others are wrong

→ A ❌ Never act on urgent financial requests without verification.

→ B ❌ Email replies can be intercepted or spoofed by scammers.

→ D ❌ Ignoring is safer than complying, but verification is always best.

QUESTION 3 OF 6

Suspicious Email Attachment

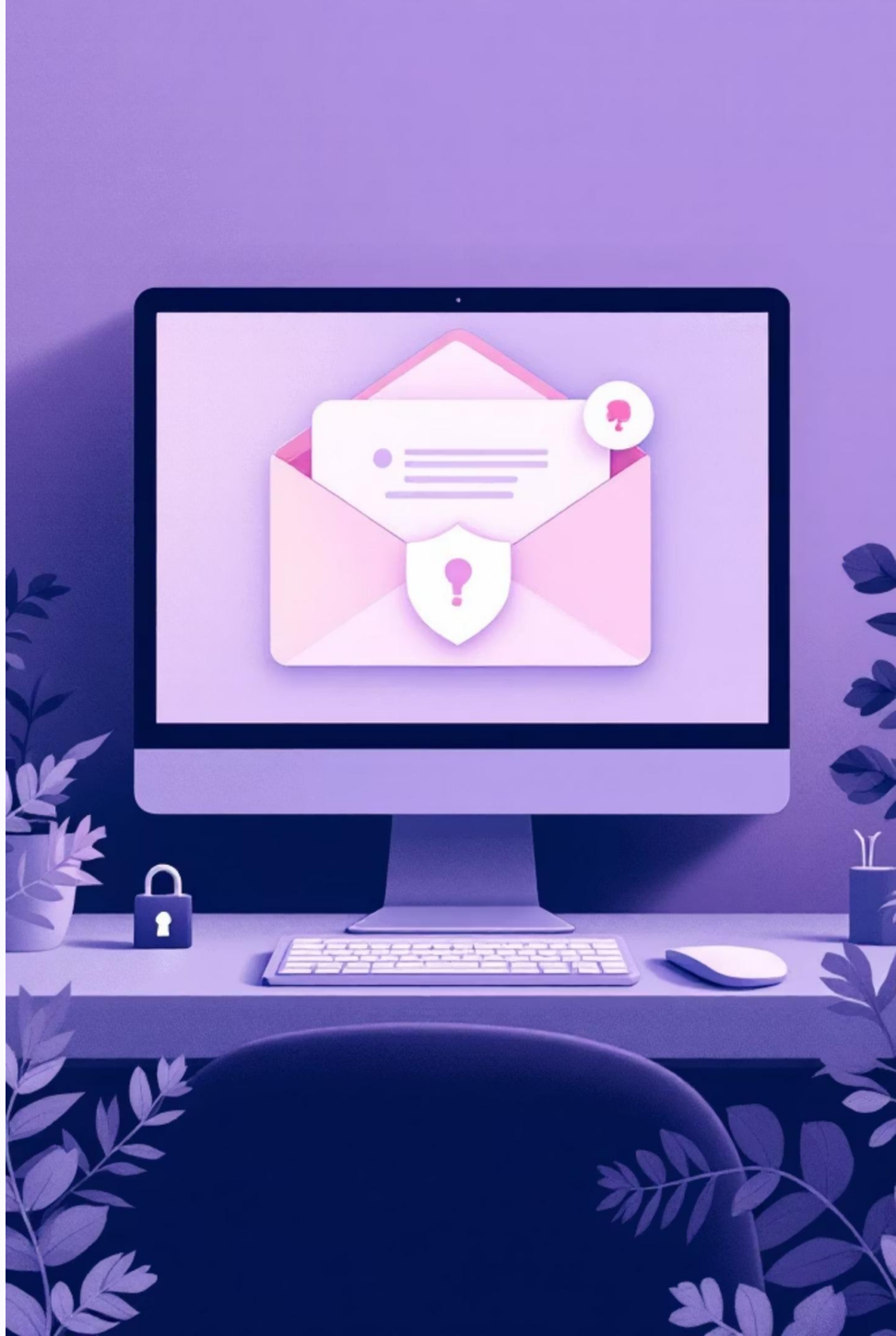
What is the safest way to handle a suspicious email attachment?

A
Open it to check its contents

B
Delete it immediately without investigation

C
Scan it with antivirus software before opening

D
Forward it to coworkers to ask if it's safe



ANSWER — QUESTION 3

Suspicious Email Attachment

A ❌

Opening it could silently **execute malware** on your device.

B ❌

Deleting without reporting means **IT misses a threat** that could affect others.

C ✔

Scanning with antivirus software **detects threats before they activate.** Then report it to IT.

D ❌

Forwarding a malicious file **spreads the threat** across your organization.

Best Practice: Scan → Report to IT → Delete. Never open or forward unknown attachments.

QUESTION 4 OF 6

Spotting a Phishing Email

What is the best way to identify a phishing email?

A
Click the link to verify the sender

B
Check the sender's email address and look for typos

C
Respond quickly to avoid losing access

D
Forward it to friends for their opinions

ANSWER — QUESTION 4

Spotting a Phishing Email

✔ Correct Answer: B

Check the sender's email address carefully and look for **subtle typos, misspellings, or unusual domains** — these are hallmarks of phishing attempts.

→ A ❌ Clicking can redirect you to a convincing fake site.

→ C ❌ Urgency is a manipulation tactic — slow down.

→ D ❌ Forwarding may spread a malicious message.

QUESTION 5 OF 6

IT Department Impersonation

A caller claims to be from IT and asks for your login credentials. What do you do?

A
Provide them immediately

B
Ask them to email you first

C
Verify their identity with IT before responding

D
Ignore them

ANSWER — QUESTION 5

IT Department Impersonation

A ❌

IT departments never ask for passwords. Sharing credentials is always a red flag.

B ❌

A scammer can **spoof email addresses** just as easily as phone numbers.

C ✔

Hang up and contact IT directly using an official number. Always confirm before responding to credential requests.

D ❌

Ignoring could **delay a legitimate security alert.** Report suspicious calls to IT instead.

Golden Rule: No legitimate IT professional will ever ask for your password — over the phone, by email, or in person.

QUESTION 6 OF 6

Finding an Unknown Device

You see a USB Drive labeled "Confidential Salaries" in the parking lot. What should you do?

A
Plug it into your computer to check

B
Leave it there

C
Hand it to security

D
Keep it as a souvenir

ANSWER — QUESTION 6

Finding an Unknown Device

❌ A) Plug it in to check

Unknown USB drives can silently **install malware or ransomware** the moment they're connected — no click required.

❌ B) Leave it there

Leaving it unattended means anyone else could pick it up and plug it in, **spreading the risk** to your whole network.

✔ C) Hand it to security

The correct answer. **IT and security can safely inspect**, contain, and dispose of the device without risk to company systems.

❌ D) Keep it as a souvenir

Holding onto an unknown device is unsafe. **It may be booby-trapped** and you'd still be responsible if it caused harm.

Key Takeaway: Dropped USB drives are a classic social engineering tactic. When in doubt, don't plug it in — hand it to security immediately.