End-User Security Fundamentals

Essential security awareness for every employee

CosmicBytez Labs • Security Awareness Training • 2026

Notes: Welcome the audience. This deck covers the 8 core modules every employee should complete.

Module 1: Phishing & Social Engineering

- Phishing is the #1 attack vector — responsible for 90%+ of breaches
- Attackers use email (phishing), phone (vishing), and text (smishing)
- Look for: urgency, mismatched domains, generic greetings, suspicious links
- STOP → LOOK → THINK before clicking any link
- Report every suspicious message — no penalties for false alarms

> If it feels urgent and unexpected, it is probably a phish.

Notes: Cover real-world examples. Show a side-by-side of legitimate vs phishing email.

Module 2: Password Hygiene & MFA

- Use unique 16+ character passphrases for every account
- A password manager is non-negotiable — Bitwarden, 1Password, KeePass
- Enable MFA everywhere: hardware keys > authenticator apps > SMS
- Never share credentials via email, chat, or sticky notes
- Check haveibeenpwned.com for compromised accounts

> MFA blocks 99.9% of automated credential attacks.

Notes: Demo a password manager. Show the difference between weak and strong passwords.

Module 3: Safe Browsing & Downloads

- Always verify HTTPS and the domain name before entering credentials
- Download software only from official, verified sources
- Use an ad blocker to prevent malvertising attacks
- Be skeptical of pop-ups: "Your computer is infected!" is always a scam
- Keep browsers and extensions updated — enable auto-update

Notes: Show examples of malicious download pages vs legitimate ones.

Module 4: Physical Security Awareness

- Lock your workstation: Win+L (Windows) or Ctrl+Cmd+Q (Mac)
- One badge, one person — never hold doors for tailgaters
- Position screens away from public view
- Shred sensitive documents — never use regular recycling
- Report unescorted visitors in secure areas

Notes: Ask: "Who has their screen lock set to auto-lock?" Encourage immediate action.

Module 5: Data Handling & Classification

- Four levels: Public, Internal, Confidential, Restricted
- Restricted data requires encryption at rest and in transit
- Use only approved platforms for sharing sensitive files
- Apply "need to know" — share only with authorized individuals
- Follow data retention policies — delete when no longer needed

Notes: Give examples of each classification level using real document types.

Module 6: Removable Media & USB Safety

- Never plug in unknown or found USB drives
- USB drop attacks: attackers leave infected drives in common areas
- Use only company-approved, encrypted USB devices
- Disable autorun/autoplay on all systems
- Found a drive? Bag it and deliver to IT Security

> One USB drive took down Iran's nuclear centrifuges (Stuxnet). What could it do to your network?

Notes: Reference the Stuxnet case study. Show how a USB Rubber Ducky works.

Module 7: Remote Work Security

- Always-on VPN for all company resource access
- Secure home Wi-Fi: WPA3, strong password, updated firmware
- Separate work devices from personal devices
- Full-disk encryption on all work laptops (BitLocker / FileVault)
- Dedicated workspace with screens not visible to others

Notes: Ask who works remotely. Discuss common home network vulnerabilities.

Module 8: Reporting Suspicious Activity

- Report immediately — even if unsure
- Preserve evidence: do not delete or modify suspicious messages
- Use designated channels: Report Phishing button, security hotline, ticket system
- Document: time, what happened, files/links involved
- No penalties for false alarms — under-reporting is the real risk

Notes: Walk through the reporting process step by step. Show the Report Phishing button in Outlook.

Key Takeaways

- Think before you click — verify every link and sender
- Use strong, unique passwords with MFA on every account
- Lock your screen, clean your desk, shred your documents
- Report anything suspicious — you are the first line of defense
- Security is everyone's responsibility, not just IT's

> Complete your training modules and earn your security awareness certificate at labs.cosmicbytez.ca/training

Notes: Summarize the key message: every employee is a security sensor. Point them to the training platform for certification.

Questions & Answers

Thank you for your commitment to security awareness.

Notes: Open the floor for questions. Have backup slides ready for common questions about password managers, VPNs, and reporting.