Cybersecurity Awareness Training: Protecting Your Workplace

Target Audience: Employees from different departments who require basic cybersecurity awareness training.

Course Learning Objectives:

1. Identify at least three common cybersecurity threats by correctly categorizing real-world examples with 80% accuracy in an interactive assessment.
2. Recognize at least three cybersecurity best practices in a simulated workplace scenario, achieving a success rate of 80% or higher.
3. List the appropriate steps for responding to security incidents and reporting suspicious activity in a simulated case study, achieving at least 85% accuracy.

Introduction (Engaging Opening)

- Animated video or scenario: An employee receives an email from the IT department that seems suspicious. What should the employee do?
- Learning objectives overview
- Interactive checklist: What are your current knowledge gaps in the field of cybersecurity?

Module 1: Understanding Cyber Threats

- Interactive infographic: Overview of common threats phishing, malware, ransomware, social engineering).
- Mini-game: Drag and drop exercise matching threats with their corresponding definitions.

Module 2: Phishing & Social Engineering Defense

- Scenario-based simulation: Users receive either an email or a phone call and must decide whether it’s a phishing attempt or not.
- Branching decision making activity: Users can choose how to respond to suspicious emails and receive feedback based on their selections.

Module 3: Safe Password & Device Practices

- Password strength checker: interactive tool where users test different password combinations.
- Best practices for multi-factor authentication (MFA) and device security.

Module 4: Reporting & Incident Response

- Interactive case study: A security breach occurs, how should the employees react to the situation?
- Knowledge Check: Create a few questions based on a security breach, and let the user select the correct actions based on different cyber incidents.

Conclusion & Certification

- Recap of key takeaways.
- Final Knowledge Check (80% required to pass)
- Digital certification for successful completion.

Prototype Outline for Articulate Storyline Development

Introduction (Engage & Set Expectations)

Opening Scenario (Animated Video/Interactive Story)

- Employee receives a suspicious email from IT support requesting login credentials.
- Employee's need to choose how to respond to the suspicious email (Branching Interaction).

Learning Objectives (Animated Text + Voiceover)

1. Identify at least three common cybersecurity threats by correctly categorizing real-world examples with 80% accuracy in an interactive assessment.
2. Recognize at least three cybersecurity best practices in a simulated workplace scenario, achieving a success rate of 80% or higher.
3. List the appropriate steps for responding to security incidents and reporting suspicious activity in a simulated case study, achieving at least 85% accuracy.

Pre-Assessment (Knowledge Check)

- Learners categorize different cybersecurity threats before starting.

Which of the following is the best reason why cybersecurity awareness is important in the workplace?
a. To avoid annoying security pop-ups
b. To reduce IT department workload
c. To protect sensitive data and prevent costly breaches
d. To make internet browsing faster

Module 1: Understanding Cyber Threats

Learning Objective: Identify at least three common cybersecurity threats, phishing, social engineering, and malware/ransomeware.

Interactive Infographic (Clickable Threat Types)

Each icon (phishing, social engineering, Malware/Ransomware) opens a short interactive learning scene, with example and mini-challenges.

What is Phishing?

Fraudulent emails that appear legitimate, attempting to trick users into clicking malicious links, downloading attachments, or entering personal credentials.Provide a few examples of fake emails containing malicious links that learners may encounter. Fraudulent messages attempting to trick recipients into revealing sensitive information.

Mini Scenario 1

A learner receives an email that appears to be from the IT department.

Subject: "URGENT: Your Password Will Expire Today!"

Options:

Click the link
Hover to check URL
Report to IT

Mini Scenario 2

An email from a vendor, attached with an invoice, was sent to me.

Attachment name: Invoice_Q1_2025.docx.exe

Prompt: "What should you do before opening?"

Feedback highlights hidden file extensions and scanning tools.

Red Flags to Teach:

- Urgent language or threats
- Unusual sender address
- Suspicious URLs or attachments
- Generic greetings ("Dear User")

Interactive Element: Drag and drop email red flags onto a sample email interface.

What is Social Engineering?

The use of deception to manipulate individuals into giving away confidential or personal information, often through impersonation or emotional appeal.

Common Tactics

- Pretexting (pretending to be someone in authority)
- Tailgating (following someone into a secure building)
- Baiting (leaving a malware infected USB in a public space)
- "CEO Fraud" or "Boss Email Scams"

Mini Scenario

A learner receives a Teams message from “HR” requesting their payroll login credentials for an urgent audit.

What should you do?
a. Verify the message source
b. Provide the information due to the "urgent" tone

What exactly is Malware and Ransomware?

Malicious software, also known as malware, is designed to cause damage, disrupt systems, or gain unauthorized access to sensitive data.

Examples of Malware and Ransomware:

- Viruses: Attach to clean files and spread uncontrollably.
- Trojans: Disguise software as legitimate to deceive users into installing it.
- Ransomware: Encrypts data and requires payment.
- Spyware: Gathers user information without their consent, silently.

How Learners May Encounter Malware and Ransomeware:

Downloading files from untrusted sources, clicking ads on shady websites, using infected USBs or software, and ignoring software or security updates are all ways to compromise your security.

Mini Scenario

A pop up offers a "free system scan." After downloading, the systems slows down and personal data is accessed.

Learners must identify the reasons behind the errors.

Mini Game (Drag & Drop Exercise)

Learners will match cybersecurity threats types with examples.

Knowledge Check

Which of the following is a sign of a phishing email?

c. Comes from a known sender with a greeting
d. Requests urgent action and includes suspicious links
e. Includes your name and contact details
f. Has a secure attachment

Social engineering relies on:

a. Computer code
b. Network failures
c. Human manipulation
d. Antivirus software

What does malware typically do?

a. Helps speed up internet performance
b. Enhances software security
c. Damages, disables, or steals data from your system
d. Encrypts files for protection

Module 2: Defending Against Phishing & Social Engineering

Learning Objective: Identify and respond to at least two simulated phishing attempts and one social engineering scenario.

Key Concepts

Phishing emails are often filled with visual and contextual clues that can help alert users. Teach them to spot the following:

- Generic greetings (Dear User, Hello Sir/Madam)
- Spelling and grammar mistakes (Pleese update your account immediatly)
- Suspicious or mismatched links (Hovering over a link shows an unexpected URL)
- Urgent or threatening language (Your account will be deleted!)
- Unusual sender addresses (e.g. **it.support@company-update-security.com**)

Voice Phishing (Vishing) & Impersonation

Voice phishing and impersonation scams are social engineering tactics that employ real-time communication to establish trust and obtain sensitive information.

Common Tactics

1. Caller impersonation (IT, HR, CEO, or vendor)
2. Uses urgency or panic (We're updating your payroll, we need your information now)
3. May use spoofed numbers or names
4. Asks for sensitive data (login credentials, financial information)

Real World Example:

"Hi, this is Mark from IT. We noticed an issue with your email and need to verify your username and password to fix it remotely."

Scenario Based Simulation (Email & Phone Scam Detection)

Learners review an email and a call transcript, then choose the best response from the branching options.

Learners review a simulated phishing email and decided:

- **Report as phishing**
- Click the link
- Reply with personal information

Learners experience a simulated phone scam:

- Provide sensitive information
- **Verify caller identity**
- Ignore the call

Branching Feedback (Personalized Responses)

- Correct: Reinforces best practices
- Incorrect: Provides immediate feedback and guidance

Verifying Senders & Reporting Suspicious Content

Take proactive steps to verify the authenticity of emails, calls, or messages before taking any action.

Verification Methods

1. Hover over links to check URLs
2. Contact the sender via official channels (e.g., call IT directly)
3. Check internal directories or intranet portals
4. Use security tools to scan suspicious attachments

Reporting Best Practices

1. Use the "Report Phishing" feature in email clients
2. Notify your IT or Security Team with details or screenshots
3. Do not forward suspicious messages to colleagues

Quick Decision Mini Game: Phishing & Social Engineering

A series of message or emails. Please choose whether to verify, report or ignore.

One message or email appears on screen at a time
Learner selects Verify, Report or Ignore
Immediate feedback appears based on which option is chosen

Scenario 1: Suspicious Email from Payroll Support

Subject: Action Required: Payroll Verification
From: payroll-support@secure-payrolls.net

_"Hello Team,
Please confirm your payroll info by clicking the secure link below.
All employees must complete this today to avoid paycheck delays.

[Confirm Info Here]"_

Verify: Correct. Contact Payroll or HR directly to confirm if this email is legitimate.

Feedback: It's a great choice. Always verify urgent financial requests with official sources. This message used urgency and a lookalike domain to deceive users.

Report: Also Correct. Use the Report Phishing button in your email client.

Feedback: Great job! However, this email raises several red flags, including a suspicious sender domain and a sense of urgency to act quickly.

Ignore: Incorrect!

Feedback: Even if you don't click on suspicious emails, ignoring them can prevent threats from being reported. Always take action, verify the email, or report it.

Scenario 2: Teams Message from IT Help Desk

Teams Simulation

IT Help Desk - Urgent

Hey, we're running a network update and need your login information to reconnect your access. Can you send it over real quick?
(Sent via internal chat tool via Teams)

Verify: Correct. Call or message the IT department through official contact information.

Feedback: Yes! Internal messages can be spoofed or sent from compromised accounts. Always confirm through trusted channels.

Report: Correct.

Feedback: Excellent response. Even though it looks internal, this request is suspicious and should be flagged.

Ignore: Incorrect

Feedback: Ignoring suspicious messages without alerting IT puts your company at risk. Take action to protect your team.

Knowledge Check

If you receive and email asking you to click a link to reset password unexpectedly, you should:

a. Click the link immediately
b. Forward it to your manager
c. Verify it through a separate secure source or report it
d. Ignore it

In a phone call, someone claims to be IT support and asks for you login. You should:

a. Give it if they sound credible
b. Ask for their name and call back through official channels
c. Ignore it
d. Record the call

Which action helps verify if an email link is safe?

a. Forwarding it to your coworker
b. Hovering over the link to inspect the destination URL
c. Copy pasting the link in your browser
d. Clicking the link to "test" it

Module 3: Safe Password & Device security

Learning Objective: Apply at least three cybersecurity best practices creating strong passwords, enabling multi-factor authentication, and securing their devices by identify risky behaviors.

Password Complexity

- **Password Length:** 12+ characters.
- **Password Complexity:** Include uppercase, lowercase, numbers, and special characters.
- **Password Reuse:** Never reuse passwords across multiple sites.

Interactive Activity: Password Strength Tester

Enter a sample passwords to see how secure they are.

Visual: Simple password input field on-screen
Action: Type in a sample passwords to get feedback (e.g., red/yellow/green strength meter)

Feedback examples:

- Fluffy123 -> Weak: Contains common words, short length
- @R3dCar$2024! -> Strong: Includes complexity and unpredictability
- Toddedwards1 -> Moderated: Personal information, lacks symbols

Multi-Factor Authentication (MFA)

Key Points: MFA adds a second layer of security beyond just your password.

Common MFA Methods:

- Code via text/email
- Authenticator apps (Microsoft/Google Authenticator)
- Biometric login (fingerprint or face scan)

Mini Scenario

A login screen appears after typing in a password.

Prompt: Which method below would be the best second step?

1. **Send code to phone**
2. Answer security question
3. Enter birthday

Tip: Even if someone steals your password, they won't have access to your second factor!

Safe Browsing Habits

Key Points:

- Only enter data on websites with HTTPS (secure connection)
- Avoid clicking pop up ads or unfamiliar downloads
- Use VPNs when on public Wi-Fi to encrypt your connection

Micro Interaction:

Visual: Screenshot of a browser window with multiple tabs.
Task: Click on the one that's safe.

Examples:

http://example-login.com
https://mycompanyportal.com
FreeMovieHD.ex download prompt

Bonus Tip: If the padlock icon is missing, it's not safe!

Device Security Best Practices

Key Points

- Always lock your screen when stepping away.
- Enable automatic software updates to patch security flaws.
- Avoid USB drives from unknown sources.
- Don't write passwords on sticky notes or store them in browsers.

Gamified Challenge: Spot the Security Risks

Identify 5 security risks in a digital workspace.

Users click on risky behavior in an office environment (unlocked computer, password on sticky note).

1. Desktop with screen unlocked
2. Sticky note with password on monitor
3. Open USB drive labeled "confidential"
4. Expired antivirus warning on the screen
5. Browser open to a sketchy website

Click each risky behavior. Each time they click a tooltip pops up explaining:

Leaving your screen unlicked makes it easy for someone to access confidential data while you're away.

Knowledge Check

Which password is the strongest?

a. Password123
b. Qwerty
c. $T)rm!n3G@l@xy!
d. johndoe

What is multi-factor authentication?

a. Logging in twice
b. Using two or more verification methods
c. Sharing passwords
d. Using a long password

Which of the following is a security best practice?

a. Writing passwords on sticky notes
b. Connecting to public Wi-Fi without a VPN
c. Locking your screen when away from your desk
d. Disabling firewalls for faster internet

Module 4: Responding to Security Incidents

Learning Objective: Illustrate the appropriate next steps in response to simulated security breaches or suspicious activity scenarios.

Recognizing Suspicious Activity

Key Points

Suspicious activity can be subtle. Learners should be trained to spot the following:

- Unauthorized logins or access attempts (especially from unfamiliar locations/devices)
- Unexpected system behavior (slowdowns, crashing apps, mouse moving on its own)
- Unfamiliar software or new icons appearing suddenly
- Pop ups or messages demanding payment (ransomware indicators)
- Changes to security settings (firewall turned off, antivirus disabled)

Interactive Case Study (Choose Your Response)

Visual: A simulated computer desktop
Task: Learners click on items they believe are suspicious

Correct examples include:

1. Login alert from Russia at 3 AM
2. Antivirus disabled message
3. A new application called SpeedBoosterX installed
4. System is infected! Call support now! Pop up

A user encounters an unusual system alert. They must decide whether to report it, ignore it, or investigate it.

Feedback per click: Correct: That pop-up is a common tactic used in tech support scams.

Reporting a Security Incident

Key Points

- Who: Always report to the IT department, Security team, or through official internal systems.
- How: Use company provided tools (security ticketing system, dedicated email, or call in support)
- When: Immediately, time is critical to contain threats.

Interactive Case Study: Choose Your Response

Scenario 1: Suspicious System Alert

You return from lunch and find your screen showing:

Your system has been infected. Click here to run a free scan.

Choices:

- Report it to IT immediately: Feedback Correct. You've spotted a classic fake antivirus alert. Quick reporting helps prevent malware spread.
- Ignore it and close the alerts: Feedback: That's risky. Even closing it may activate hidden malware. Always report first.
- Click to investigate and scan your system: Feedback: That might trigger malicious downloads. Trust your IT team to handle it safely.

Scenario 2: Unauthorized Login Alert

You receive an email from your company's login alert system:

Your account was accessed from a new location: Ukraine. Was this you?

Choices:

- Change your password immediately and report it: Feedback: Correct! Resetting your password and notifying IT helps stop further unauthorized access.
- Assume it's a mistake and do nothing: Feedback: Doing nothing could result in data theft or account compromise.
- Forward the email to a coworker for advice: Feedback: Always go directly to your IT or security team. Forwarding may spread sensitive information.

Why Quick Reporting Matters

Key Points

- Cyber incidents escalate quickly: Delays can allow malware to spread, data to be stolen, or systems to be compromised.
- Early action reduces risk to the organization and protects your team.
- Most breaches begin with small warning signs, acting early is the best defense.

Example Statistic Slide:

Over 60% of data breaches are discovered days or weeks after the initial intrusion. (Source: IBM X-Force Threat Intelligence Index)

Knowledge Check

What's the first thing you should do if you notice suspicious activity on your device?
a. Try to fix it yourself
b. Keep working as usual
c. Immediately report it to your security team
d. Unplug your device

Why is quick reporting important in cybersecurity?
a. It helps avoid blame
b. It allows security teams to act fast and limit damage
c. It reduces paperwork
d. It notifies HR

Which of the following should be reported?
a. Forgotten password
b. Unusual pop-ups and new software you didn't install
c. Low battery warning
d. Receiving an office memo

Final Assessment (SCORM Tracked Quiz, 85% Required to Pass)

Which of these is an example of phishing?
a. A verified app update
b. An email from IT with a suspicious link and urgency

You find a USB stick in the parking lot. What do you do?
a. Plug it in to check its content
b. Give it to IT/security

Match the threat to the description:

Phishing -> Fake emails for data
Malware -> Harmful software
Social Engineering -> Tricking people into

Your coworker shares their password with you. You should:
a. Use it carefully
b. Report it as a violation

Which is the most secure password?
a. 123456
b. !Q3$sd8#Lp09
c. Abc123
d. Yourname

What does MFA stand for?
a. Major Firewall Alert
b. Multi-Factor Authentication
c. Multiple Failed Access
d. Manual File Approval

During a call, someone urgently asks for your login info. You should:
a. Provide it
b. Hang up and report the call

A pop-up appears asking for admin credentials. You weren't expecting it. What should you do?
a. Enter your credentials
b. Report it immediately

What should you check before clicking on a link in an email?
a. Font style
b. Sender address and link destination
c. Subject line
d. Emoji user

What does HTTPS mean?
a. Secure, encrypted website
b. Fast website
c. Hacker Tracking System
d. Hosted by Telecom Provider

Conclusions: Stay Cyber Smart

Well Done! You've Completed the Cybersecurity Awareness Training

You've taken a big step in protecting yourself, your team, and your organization from cybersecurity threats.

Key Takeaways:

1. Recognize Threats:
   - Phishing, social engineering, and malware can appear in everyday message and files.
   - Always look for red flags, urgency, suspicious links, unknown senders.

2. Secure Your Access:
   - Use strong passwords (12+ characters, symbols, unpredictability).
   - Enable multi-factor authentication on all critical accounts.
   - Keep your devices and software updated.

3. Respond Quickly:
   - If something feels off, report it immediately, even if you're unsure.
   - Never ignore alerts, unexpected logins, or pop ups.

Call to Action:

Security starts with you. Make cybersecurity a daily habit, stay alert, think critically, and speak up when something seems wrong.

Next Steps:

1. Download Your Certificate
2. Bookmark our Cybersecurity Resource Hub (if applicable)
3. Encourage your team to complete the training too!

Completion Badge & Digital Certificate

Upon passing the assessment, learners will receive a customized certificate.

CYBERSECURITY
AWARENESS
TRAINING
Completd