techclass

# THE ULTIMATE CYBERSECURITY AWARENESS CHECKLIST ✓

A practical guide for HR and L&D managers to plan, implement, and measure cybersecurity awareness programs that protect their workforce and organization.

# Table of Contents


Introduction 03

Phishing & Scams 04

Passwords & MFA 05

Email & Messaging 06

Web & Downloads 07

Work Devices 08

Mobile & Remote 09

Data & Privacy 10

Malware & Ransomware 11

Physical Security 12

Social Media & Reputation 13

Conlusion 14

techclass

# Introduction

## Why Cybersecurity Awareness Training Matters?

Cybersecurity incidents often start with a simple human mistake: a clicked phishing link, a reused password, or a mishandled file. This checklist helps you design or evaluate your cybersecurity awareness training by focusing on the core concerns that employees should understand and manage in their daily work.

This checklist is designed for HR, L&D professionals, compliance officers, and team managers who are responsible for planning, buying, or implementing cybersecurity training programs. Use it to review your current training content, identify gaps, and ensure critical risks are properly addressed.

**Disclaimer:**
The information provided in this eBook is intended for educational purposes and general guidance only.

techclass

# Phishing & Scams

→ Covers how well people recognize and mentally flag deceptive messages.

## List of checklist items

- [ ] **Phishing email basics**

  Recognizes that emails can be fabricated to steal logins, money, or information, especially as sophisticated phishing simulations increasingly mirror the tactics employees may face in real inboxes.

- [ ] **Red flags in messages**

  Notices odd senders, tone, links, and requests that don't feel right.

- [ ] **Suspicious links and attachments**

  Treats links and attachments as potentially risky, not automatically harmless.

- [ ] **Fake login pages**

  Understands that sign-in pages can be cloned to capture credentials.

- [ ] **Urgent or "authority" scams**

  Sees urgent requests "from the boss" or "from a bank" as something to verify, not obey blindly.

- [ ] **Phone/SMS scams (vishing & smishing)**

  Views calls and texts asking for codes, passwords, or payments as suspicious.

- [ ] **Reporting suspicious messages**

  Treats strange messages as something to report, not just delete and forget.

# Passwords & MFA

→ Focuses on how people secure accounts and logins as part of broader efforts to train employees on cybersecurity and connect daily habits to organizational protection.

## List of checklist items

- [ ] Strong password/passphrase requirement

  Accepts that short or simple passwords are easy to guess or crack.

- [ ] No password reuse

  Understands that reusing one password lets a single breach unlock multiple accounts.

- [ ] No password sharing

  Recognizes that shared passwords hide accountability and invite misuse.

- [ ] Secure password storage

  Sees passwords left in notes, chats, or documents as exposed secrets.

- [ ] Password manager usage

  Views a well-protected password vault as safer than scattered, ad-hoc storage.

- [ ] MFA requirement for key systems

  Accepts a second factor as a crucial barrier when passwords leak.

- [ ] Access changes over time

  Accepts that credentials and access levels should change when roles, projects, or employment status change.

techclass

# Email & Messaging

→ Covers everyday communication behaviors that can leak data or create openings.

## List of checklist items

- [ ] **Checking recipients before sending**
  Understands that one wrong address can expose sensitive information.

- [ ] **Handling sensitive information**
  Recognizes that some details are too sensitive for casual email or chat.

- [ ] **Misdirected email as an incident**
  Treats sending data to the wrong person as a security event, not a minor typo.

- [ ] **Forwarding externally**
  Realizes that forwarding threads can reveal old attachments and hidden context.

- [ ] **Use of chat/collaboration platforms**
  Does not treat internal chat as a safe place for passwords or confidential data.

- [ ] **Reporting messaging errors or concerns**
  Views misdirected or suspicious messages as issues that should be raised promptly.

- [ ] **Managing attachments carefully**
  Shares only necessary files, checks attachments before sending, and avoids spreading outdated or unnecessary data.

techclass

# Web & Downloads

→ Covers awareness of online risks from sites, content, and downloads.

## List of checklist items

- [ ] **Recognizing risky websites**
  Accepts that some websites exist primarily to trick visitors or deliver malware.

- [ ] **Blocked sites and categories**
  Understands that blocked categories signal higher risk, not just inconvenience.

- [ ] **Approved download sources**
  Trusts official stores and company channels over random download buttons.

- [ ] **Pop-ups and fake alerts**
  Treats sudden “you’re infected” or “update now” pop-ups as traps.

- [ ] **Official update channels only**
  Recognizes fake update prompts as a common way to install malicious software.

- [ ] **Browser extension rules**
  Sees extensions as powerful components that can spy, steal, or alter content.

- [ ] **Personal browsing boundaries**
  Understands that certain browsing habits greatly increase exposure to infection.

techclass

# Work Devices

→ Covers physical and digital habits around company laptops and desktops.

## List of checklist items

- [ ] Locking screens when away

  Accepts that an unlocked workstation is essentially open access to all its data.

- [ ] Automatic screen lock

  Treats timeouts as a safety net rather than an obstacle to productivity.

- [ ] Physical care and storage

  Recognizes that a stolen device often includes saved files and credentials.

- [ ] Allowing updates to install

  Understands that postponing updates leaves known holes open for attackers.

- [ ] Approved software only

  Sees unapproved tools as potential carriers of malware or backdoors.

- [ ] USB/removable media usage

  Treats unknown or free USB drives as suspicious, not convenient.

- [ ] Reporting unusual device behavior

  Views persistent crashes or strange pop-ups as possible signs of compromise.

# Mobile & Remote

→ Covers risks that appear when work happens on the move or outside the office, where the realities of training a remote workforce make clear guidance, repetition, and accessible learning especially important.

## List of checklist items

- [ ] Locking mobile devices
  Recognizes that an unlocked phone or tablet exposes email and work apps.

- [ ] Use of personal devices (BYOD)
  Understands that personal devices can become weak links if left unsecured.

- [ ] Approved work apps/profiles
  Accepts that only vetted apps and managed profiles should handle work data.

- [ ] VPN use for remote access
  Sees that open connections on untrusted networks expose traffic to others.

- [ ] Public Wi-Fi precautions
  Treats free Wi-Fi as a place where someone might watch or alter connections.

- [ ] Handling work documents at home
  Recognizes that printed files and notes at home can be misplaced or read by others.

- [ ] Lost or stolen devices
  Understands that each missing laptop or phone represents a potential breach.

# Data & Privacy

→ Covers how sensitive, personal, and business-critical information is perceived, reinforcing the core elements every data protection training program should make practical for employees.

## List of checklist items

- [ ] What counts as sensitive/personal data
  Recognizes that everyday records like names, IDs, histories, have real value to attackers.
- [ ] Data classification basics
  Understands some information is low impact if exposed, while other types are highly damaging.
- [ ] Storage in approved systems
  Sees random folders, local drives, or ad-hoc locations as weak places to store critical data.
- [ ] Sharing only with authorized recipients
  Accepts that giving access “to everyone” increases the chance of misuse.
- [ ] No copying to personal systems
  Understands moving work data to personal accounts or devices breaks protection controls.
- [ ] Printing and document handling
  Treats printed pages as sensitive objects that can be lost, copied, or photographed.
- [ ] Retention and deletion overview
  Recognizes that keeping data indefinitely increases damage if a breach occurs.

techclass

# Malware & Ransomware

→ Covers understanding of malicious software and its impact on systems and data.

## List of checklist items

- [ ] What malware is at a high level
  Understands that malicious software can spy, steal, disrupt, or silently alter systems.
- [ ] Common infection routes
  Recognizes that one unsafe click, download, or USB can compromise a device.
- [ ] Signs something may be wrong
  Interprets unusual behavior, slowness, pop-ups, crashes, as possible intrusion.
- [ ] Basics of ransomware
  Understands that ransomware encrypts files and demands payment to unlock them.
- [ ] Data theft before encryption
  Realizes that attackers often steal copies of data before locking systems.
- [ ] Spread across systems
  Accepts that a single infected machine can rapidly affect many others.
- [ ] Need for quick escalation
  Recognizes that delayed response allows malware to deepen and widen its impact.

# Physical Security

→ Covers how physical access is viewed as part of cybersecurity.

## List of checklist items

- [ ] **Badge and key responsibilities**
  Understands that misplaced or borrowed access devices can turn outsiders into insiders.

- [ ] **Tailgating prevention**
  Recognizes that letting unknown people follow through secure doors is a real risk.

- [ ] **Visitor registration and escort**
  Sees untracked visitors as blind spots inside controlled areas.

- [ ] **Clean desk standard**
  Accepts that visible papers and devices can be read, photographed, or taken.

- [ ] **Locked storage for sensitive documents**
  Understands that unlocked cabinets or boxes invite unauthorized browsing.

- [ ] **Secure printer behavior**
  Treats uncollected printouts as exposed information, not harmless leftovers.

- [ ] **Lost badge/key reporting**
  Recognizes that failing to report lost access items extends the opportunity for misuse.

techclass

# Social Media & Reputation

→ Covers awareness of how online activity can expose the organization or its data.

## List of checklist items

- [ ] Guidelines for sharing about work

  Recognizes that casual updates can reveal sensitive clients, projects, or internal details.

- [ ] Restrictions on photos and screenshots

  Understands that visible screens, badges, and documents in photos can leak information.

- [ ] Posting locations and travel

  Sees real-time location or travel posts as useful intelligence for targeting.

- [ ] Handling contact requests from unknown people

  Treats unexpected “friendly” approaches as potential reconnaissance or scam attempts.

- [ ] Use of official company accounts

  Accepts that posts from corporate channels carry high impact and must be tightly controlled.

- [ ] Common social media scam patterns

  Recognizes fake support, malicious links, and too-good-to-be-true offers as threat vehicles.

- [ ] Reporting impersonation or online issues

  Views fake profiles and hostile activity as risks that should be escalated quickly.

# Conlusion

## 01.

### A Guide, Not a Rulebook

Use this checklist as a starting point to review training content, not as a rigid security rulebook.

## 02.

### Customize for Your Organization

Adapt each item to your industry, risk level, culture, tech stack, and compliance needs, including NIS2-compliant cybersecurity training

## 03.

### Make Cybersecurity Practically Relevant

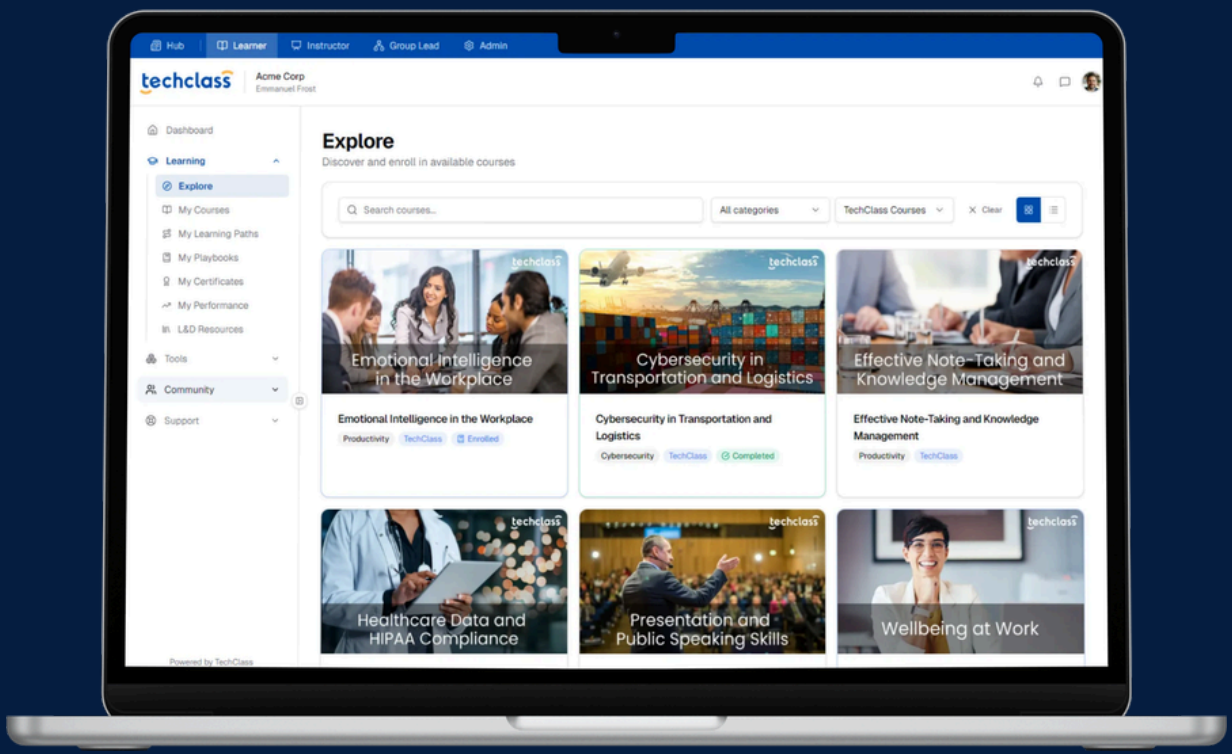
Anchor topics in real tasks, systems, and decisions so people clearly see how these cyber risks show up in their day-to-day work and why their behavior matters.

Accelerate Your Workforce Development

# Book Your Free Demo Session

**BOOK NOW**

techclass.com/demo




## #1 All-in-One Employee Onboarding and Training Platform

techclass

sales@techclass.com