Internet Security Training Catalog

Cybersecurity - AI Slop

AI-generated content is making cyber threats faster, cheaper, and far more convincing. This course helps learners understand how low-quality but highly persuasive AI-generated emails, messages, fake profiles, documents, and web content are being used to manipulate trust, spread misinformation, and support phishing and fraud. It focuses on the growing reality that employees can no longer rely on tone, grammar, or polish alone to judge whether something is legitimate.

Learners will explore how AI-generated “slop” shows up in business communication, how attackers use it to imitate vendors, executives, and coworkers, and what warning signs still matter when the content looks believable at first glance. The course helps organizations strengthen employee skepticism, improve verification habits, and reduce the risk that someone clicks, shares, approves, or responds to something dangerous simply because it looked credible enough.

Cybersecurity - Basics

Cybersecurity failures often begin with ordinary moments such as opening the wrong attachment, reusing a password, clicking a fake login page, or ignoring a small warning sign. This course gives learners a practical foundation in the most common cyber risks facing today’s workforce and explains why everyday employee behavior plays such a major role in whether an organization stays secure or becomes exposed. It is designed to make cybersecurity understandable, relevant, and immediately useful for non-technical employees.

Learners will explore core topics such as phishing, password hygiene, safe browsing, device security, suspicious links, social engineering, and the importance of reporting issues early. The course helps organizations create a stronger security culture by giving employees the awareness and habits they need to recognize risk sooner, make better decisions in the moment, and act as a more reliable first line of defense against preventable cyber incidents.

Cybersecurity - Collaboration & Cloud Hygiene

Modern work depends on shared drives, cloud platforms, messaging tools, file sharing, and collaborative workspaces, but these conveniences also create major security gaps when access, sharing, and storage are not handled carefully. This course helps learners understand how poor cloud hygiene leads to accidental exposure of sensitive files, excessive permissions, data leakage, and risky collaboration practices that quietly increase organizational vulnerability. It makes the connection between everyday convenience and real cyber exposure.

Learners will explore how to manage sharing settings, control access, avoid oversharing, handle documents more securely, and use cloud-based collaboration tools with stronger judgment. The course helps organizations reduce avoidable risk in one of the most common threat areas by teaching employees how to work efficiently in shared digital environments without exposing company data, customer information, or internal systems through careless cloud behavior.

Cybersecurity - Computer Security

Work computers hold emails, credentials, internal files, customer data, cloud access, and critical

business systems, which means a single unsecured device can become an easy entry point for a much larger incident. This course helps learners understand the day-to-day actions that protect workplace computers from misuse, compromise, and unauthorized access. It focuses on practical behaviors that matter, not technical jargon, so employees can see how their choices directly affect security.

Learners will explore safe browsing, software awareness, device locking, updates, suspicious downloads, removable media, and the risks that come from using a work computer carelessly or inconsistently. The course helps organizations strengthen endpoint security by building better habits around the devices employees use every day, reducing the likelihood that simple computer misuse turns into malware, data loss, or a broader systems breach.

Cybersecurity - Email Threats Unmasked

Email remains one of the most common and successful cyberattack channels because it relies on speed, familiarity, urgency, and trust. This course helps learners understand how email threats really work, from phishing and spoofing to impersonation, malicious attachments, fake invoices, and credential-harvesting links. It focuses on what makes email such an effective attack method and why even experienced employees can still be caught off guard when a message looks routine enough.

Learners will explore the red flags that matter, the tactics attackers use to create urgency or authority, and the habits that help verify whether a message is legitimate before taking action. The course helps organizations reduce one of their biggest attack surfaces by improving employee awareness, slowing down risky reactions, and making staff more capable of spotting threats before they lead to compromised accounts, wire fraud, or malware infection.

Cybersecurity - Emerging Cyber Threats

Cyber risk changes constantly, and many attacks succeed because employees are responding to yesterday's threats with yesterday's assumptions. This course helps learners stay current on the evolving tactics cybercriminals use, including newer forms of social engineering, AI-assisted scams, credential attacks, supply chain exposure, and increasingly sophisticated attempts to exploit fast-moving business environments. It is designed to build awareness of what is changing, not just what has always been true.

Learners will explore how the threat landscape is shifting, why attackers adapt so quickly, and what employees need to watch for as cyber tactics become more scalable, more personalized, and harder to detect. The course helps organizations stay ahead of preventable incidents by giving their workforce a more current, agile understanding of risk, making employees better prepared to respond when threats no longer look like the old examples they are used to seeing.

Cybersecurity - Malware Mastery

Malware remains one of the most damaging and disruptive forms of cyberattack because it can steal data, lock systems, monitor activity, spread silently, and shut down operations with little warning. This course helps learners understand the different forms malware can take, how it gets into an organization, and why a single unsafe click or download can lead to widespread business impact. It goes beyond the word "virus" to explain the broader malware landscape in practical terms.

Learners will explore ransomware, spyware, trojans, worms, malicious downloads, infected attachments, and the behavioral warning signs that something may already be wrong. The course

helps organizations improve prevention by showing employees how malware spreads, what unsafe behaviors create openings, and why early caution is far easier and less costly than responding after systems, files, or accounts have already been compromised.

Cybersecurity - Passwords

Passwords are one of the most basic security controls in any organization, yet weak, reused, or poorly managed passwords remain one of the easiest ways attackers gain access to systems and data. This course helps learners understand why password behavior matters more than most people think and how password shortcuts taken in the name of convenience can create serious exposure for the organization. It connects password discipline directly to account compromise, fraud, and preventable breach risk.

Learners will explore how to create stronger passwords and passphrases, avoid reuse, use password managers more effectively, and support access security with multi-factor authentication. The course helps organizations reduce a common and persistent vulnerability by making secure password practices easier to understand, easier to apply, and more clearly tied to real-world cyber risk rather than abstract IT policy.

Cybersecurity - When Malware Strikes

Knowing what malware is matters, but knowing what to do when something seems wrong is often what determines whether the incident remains contained or spreads across the organization. This course helps learners understand the immediate steps to take when malware is suspected, including how to recognize warning signs, what not to do, and why fast reporting and isolation matter so much in the early moments of an incident. It focuses on response awareness at the employee level, where timing can make a major difference.

Learners will explore common symptoms of malware, response mistakes that make infections worse, and the practical actions that help IT or security teams intervene more effectively. The course helps organizations reduce damage, shorten response time, and avoid unnecessary escalation by ensuring employees know how to respond calmly and correctly instead of hesitating, guessing, or continuing to use a compromised system.

Cybersecurity - Working Remotely

Remote and hybrid work have expanded flexibility, but they have also increased cyber risk by moving employees into less controlled environments where home networks, personal devices, public Wi-Fi, shared spaces, and informal workarounds can all create vulnerabilities. This course helps learners understand the specific cybersecurity risks tied to remote work and how everyday choices outside the office can still expose company systems, customer information, and internal communications. It makes remote security practical instead of abstract.

Learners will explore secure connections, device protection, account access, safe file handling, physical privacy, and the habits that matter when work happens outside a traditional office perimeter. The course helps organizations strengthen distributed security by giving remote employees clearer expectations and better judgment, reducing the chance that convenience, distraction, or informal remote work habits create openings for phishing, data leakage, or account compromise.