

Cybersecurity Awareness



Title	Duration (minutes)	Author	Course Description
• Foundations of Cybersecurity	4	HSI-ej4	Cybersecurity is critical in today's digital landscape. Our course "Foundations of Cybersecurity" introduces the fundamental principles of cybersecurity, including how to protect against common threats like malware and phishing. In this course, we'll also cover the tools and strategies used to safeguard systems and sensitive data.
• Cybersecurity Terminology	8	HSI-ej4	Cybersecurity is a complex topic, but everyone should be familiar with concepts like data protection policies, common cyber threats, and some proactive security measures. Understanding these fundamentals will help you safeguard sensitive information and contribute to your organization's overall cybersecurity efforts.
• Cybersecurity While Traveling	6	HSI-ej4	You should be well-aware of online hazards while you work. The threat of cyberattacks travels with you, and public spaces and networks are especially risky. Fortunately, there are many things you can do to protect yourself.
• Cybersecurity: Minimizing Insider Threats	7	HSI-ej4	According to statistics, insider threats are responsible for more than half of all data breaches. Insiders are part of the team in some way. It could be employees, vendors, third party affiliates, contractors, business partners, or former employees. It could be anyone who currently has or previously had privileged access to confidential or important data. An insider threat is the threat of malicious behaviors coming from someone who's a part of one of these insider groups. The cost to you could be enormous, so the purpose of this course is to help you minimize the risk.
• General Data Protection Regulation (GDPR)	9	HSI-ej4	The General Data Protection Regulation (GDPR) is a law in the European Union which requires leaders to have a complete understanding of what personal data is and how it's handled by their company. Safeguarding people's data privacy rights and protecting sensitive information means properly obtaining consent and following best practices for compliance.
• Cybersecurity for Remote and Hybrid Workers	9	HSI-ej4	Working remotely or in a hybrid setup has its perks, but it also means being extra careful about cybersecurity. This program explains the data safety essentials, like antivirus software, firewalls, encryption, and VPNs. It also offers practical tips on creating strong passwords, avoiding phishing scams, keeping software updated, and not mixing work and personal devices. Stay aware and follow your company's guidelines to keep everything secure.
• Using Strong Passwords	9	HSI-ej4	Cybercriminals are always one step away from controlling your files, data, and access to your accounts. This makes it crucial that you create strong, secure passwords to protect against these threats. Once you've got great passwords, tools like password managers can help you manage them, and advanced security measures like passphrases and passkeys can make them nearly impossible to crack.
• Multifactor Authentication: Making Sign-In More Secure	7	HSI-ej4	This course dives into multifactor authentication (MFA), a way to add extra security to your accounts by needing more than just a password to log in. You'll learn about common MFA methods like getting a one-time code sent to your phone, which makes it harder for anyone else to get in without your permission.
• Email Phishing	5	HSI-ej4	In this course, we'll discuss why phishing emails are so successful, what you should do if you suspect you've received a phishing email, and the steps to take if you inadvertently click on a link.
• Social Engineering	8	HSI-ej4	If you got an urgent email from your boss asking for your company's latest financial reports, what would you do? Cybercriminals can pretend to be your coworkers, using only public information, sending you emails and asking for things; if you're not careful, you might not catch the difference. This is called "social engineering", and it can have major consequences.