
Cybersecurity
integrity
Ethics & Compliance Training

integrity
Ethics & Compliance Training

Topic 1 – What Is Information Security?

1. **Video**: Information security is the art and science of preventing data from being lost or misused. Types of information that need protecting. Risks; natural events, technical failures, human error, hacking, malicious attacks.
2. **Interactive Screen**: Types of information; public, internal, confidential, restricted use.
3. **Scenario**: Identify the items in a stolen handbag that present an information security risk to the company.
4. **Key Learning**: Losing a company tablet and ID card present an information security risk for our company.
5. **Scenario**: First action to take to prevent an information security breach.
6. **Key Learning**: Actions that will minimize the damage the thieves can do should be taken immediately.
7. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 2 – Email and Messaging

1. **Interactive Screen**: Staying secure. Take care when sending emails. Always consider a more secure method. Encryption. Spam. Malware. Risks of text messaging.
2. **Scenario**: What action to take when you mistakenly use 'Reply All.'
3. **Key Learning**: Recognize the risks of restricted data falling into the wrong hands. Take responsibility for the safe dissemination of company information. Understand that you must escalate incidents through the correct channels immediately.
4. **Assessment**: Five-question quiz on the content presented in this topic.

integrity
Ethics & Compliance Training

Topic 3 – Welcome1 is Not a Password

1. **Interactive Screen**: Protecting your accounts. Strong passwords. Choosing a password. Password management.
2. **Scenario**: Identifying IT security red flags.
3. **Key Learning**: There are many strategies used for cracking passwords. The most common is 'brute force,' a method that checks every combination of letter and common words. Ensure that you use a combination of uppercase and lowercase letters, numbers, and symbols.
4. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 4 – Phishing

1. **Interactive Screen**: What is phishing? Why is it important? What are the consequences?
2. **Interactive Screen**: Types of phishing; Spear Phishing. Domain Spoofing. Malware. Keyloggers. Ransomware. Evil Twin Wi-Fi.
3. **Scenario**: Company-wide email looking for a password update.
4. **Key Learning**: Any requests for personal or confidential information should be treated with the highest degree of skepticism. Phishing tries to elicit an "act first, think later" response, based on a sense of urgency.
5. **Scenario**: Suspicious attachment.
6. **Key Learning**: Social media accounts are often an easy way to target a victim's sense of trust and curiosity. Once a hacker has control of an account, they can utilize that person's contact list to send out a broad phishing attack and potentially acquire personal data of the victim's contacts.
7. **Assessment**: Five-question quiz on the content presented in this topic.

integrity
Ethics & Compliance Training

Topic 5 – Secure Social Media

1. **Video**: How do we harness the power of social media? Your social media interactions could impact our reputation. Think before you post!
2. **Interactive Screen**: Safe practices when using social media. Conducting business communications. Privacy is not guaranteed. Accuracy of online profiles. Adopting safe practices.
3. **Scenario**: Including job details in a LinkedIn profile.
4. **Key Learning**: Most people post job titles and employer name in their social media profile. But job descriptions, colleague names, and locations should not be shared without first checking company policy.
5. **Scenario**: Social media contact with a journalist.
6. **Key Learning**: Engaging with the media regarding company business is dangerous. Always receive advice and authorization before speaking to journalists.
7. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 6 – Protect the Workplace

1. **Interactive Screen**: Security is everyone's responsibility. Guidelines on how to keep your equipment and the office secure.
2. **Scenario**: Leaving a laptop unlocked.
3. **Key Learning**: If you think your device has been breached, the first thing you need to do is contact IT Security. It takes just a minute for your computer to be breached. You must never leave your computer unlocked and unattended.
4. **Scenario**: Keeping the workplace secure.
5. **Key Learning**: Vary your routine, ensure the screen is locked when you leave your computer, use secure passwords, and be aware of your surroundings when entering through the security doors.
6. **Assessment**: Five-question quiz on the content presented in this topic.

integrity
Ethics & Compliance Training

Topic 7 – Secure Out of Office

1. **Interactive Screen**: Working remotely. Loss and theft. Data breaches. Malware threats. Storing devices and data.
2. **Scenario**: Getting online when traveling.
3. **Key Learning**: Connecting by Ethernet from a hotel room allows you to use your company laptop more securely, and using the VPN software should ensure the security of the connection. Don't take chances though.
4. **Scenario**: Sending an important document when on the road.
5. **Key Learning**: The ideal solution is to transfer files over a secure VPN connection. If you must use email, ensure that any confidential information is properly encrypted.
6. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 8 – Social Engineering and Cybercrimes

1. **Interactive Screen**: Email threats. Scams and manipulation. Cyber criminals. Social engineering.
2. **Interactive Screen**: Types of deception; physical, virtual, baiting, quid pro quo, watering hole attacks. Best practices for staying secure.
3. **Scenario**: Fake charity site.
4. **Key Learning**: It's important to verify sites to avoid malware. Often real charity events are referenced, therefore, research on the donation site should be conducted thoroughly.
5. **Scenario**: Consequences of entering credit card details on a professionally cloned site.
6. **Key Learning**: Professional cloning of websites is known as pharming and is often used in conjunction with phishing.
7. **Assessment:** Five-question quiz on the content presented in this topic.

Topic 9 – Speaking Up

1. Summary screen that wraps up the module and provides details of where to go to speak up.
2. Attestation screen where learners attest that they are ready to help keep our information secure.