SecurityIQ
BY INFOSEC INSTITUTE

Module Library

Role-Based Training for All Staff Levels, Industries and Departments

securityiq.infosecinstitute.com

INFOSEC
INSTITUTE

About SecurityIQ

SecurityIQ offers an expansive library of modules for all learner types. Content is regularly reviewed, revised and expanded by security education experts to exceed the training needs of our clients. Our training modules come in a variety of languages for multilingual, multinational teams.

A preview of all modules is available in the following pages. Each module is available in a customized format for all staff levels, industries and departments, offering you hundreds of modules to choose from to meet your training needs.

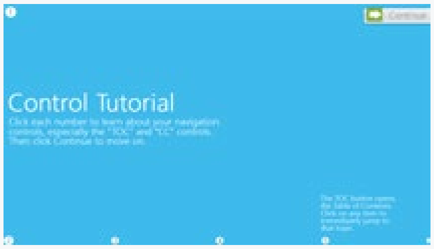
Table of Contents

Administrative Modules

Role-based customization available for all staff levels, industries and departments.

Program Introduction *(5:13 Minutes)*

In this module, we'll jump-start your security awareness training program by demonstrating and reinforcing the critical need for comprehensive cybersecurity programs in the workplace. The module will outline key areas of program focus such as cyber threats (established and emerging), recent attacks and industry regulations, and also position employees as key players in modern cybersecurity initiatives.



Control Tutorial

Click each number to learn about your navigation controls, especially the "TOC" and "CC" controls. Then click Continue to move on.

The TOC button opens the Table of Contents. Click on any item to immediately jump to that topic.

Conclusion *(2:05 Minutes)*

This module will review and reinforce critical lessons from your SecurityIQ awareness training to increase team retention of core program content.

Hackers use malware to steal, destroy, control, and launch additional attacks.

Compliance Modules

Role-based customization available for all staff levels, industries and departments.

Breach Notification

(8:14 Minutes)

This module details best practices for detecting and reporting unauthorized Protected Health Information (PHI) disclosures. Topics include HIPAA's definition of a breach, breach disclosure requirements (including the concept of "safe harbor") and recommended breach detection and notification methods.

Safe Harbor

Security Awareness Training - Breach Notification

Breach Notification for Healthcare Managers

(8:54 Minutes)

This module details best practices for detecting and reporting unauthorized protected health information disclosures. Topics include HIPAA's definition of a breach, breach disclosure requirements (including an overview of the concept of safe harbor) and recommended breach detection and notification methods. This module teaches managers how to educate their teams about breach notification policies.

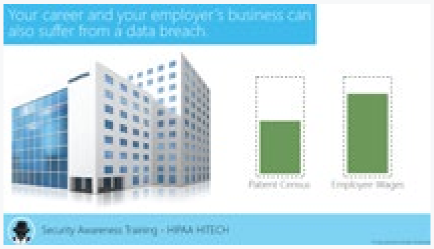
Breach Notification

Security Awareness Training - Breach Notifications for Managers

HIPAA/HITECH

(14:16 Minutes)

Our role-based HIPAA/HITECH module defines Protected Health Information (PHI), explains the need for PHI security and outlines best practices for handling PHI. We'll also suggest additional resources for PHI-related questions in the workplace



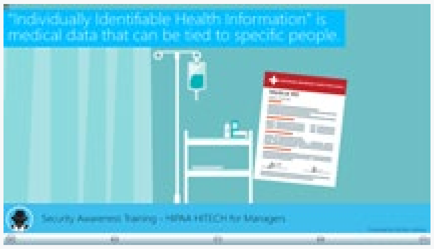
Your career and your employer's business can also suffer from a data breach.

Security Awareness Training - HIPAA HITECH

HIPAA/HITECH for Healthcare Managers

(14:21 Minutes)

This module defines protected health information (PHI), outlines best practices for handling PHI and explains the responsibilities of healthcare managers in protecting PHI and ensuring HIPAA compliance.



"Individually Identifiable Health Information" is medical data that can be tied to specific people.

Security Awareness Training - HIPAA HITECH for Managers

HIPAA/HITECH for Healthcare Executives *(14:06 Minutes)*

This module defines protected health information (PHI), outlines best practices for handling PHI, and explains the essential role healthcare executives play in protecting PHI and ensuring HIPAA compliance by implementing security policies and promoting employee training.

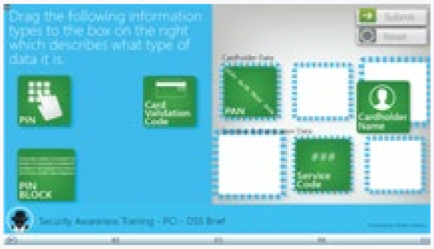
PCI-DSS *(21:43 Minutes)*

The Payment Card Industry Security Standard (PCI-DSS) regulates security standards for organizations handling branded credit cards from major vendors. This module details the training, policies and procedures required for PCI compliance, including essential cardholder data security requirements for all payment environments.

PCI DSS is issued by the Payment Card Industry Security Standards Council.

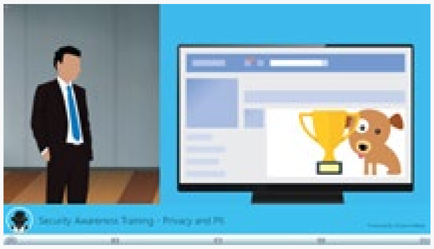
PCI-DSS Brief *(13:29 Minutes)*

This module is an abbreviated version of our core PCI-DSS training. It outlines the six main goals of the PCI-DSS, common threats and best practices for handling credit card data.


Drag the following information types to the box on the right which describes what type of data it is.

Privacy and PII *(11:31 Minutes)*

Our Privacy and PII module defines privacy and Personally Identifiable Information (PII), and reinforces the importance of data security in the workplace. Topics covered include best practices for collecting, storing, using, sharing and disposing of personal information per US government recommendations, and includes interactive team exercises for content review and reinforcement.



Privacy and PII Brief *(4:55 Minutes)*

This abbreviated version of our core Privacy and PII training will explain the basic concepts of privacy and personally identifiable information (PII). It details consequences of privacy violations, explains the purpose and importance of privacy policies and provides a brief overview of the information lifecycle.

PII is any information that can be used to identify a person.

Security Awareness Training - Privacy and PII Brief

Privacy and EU GDPR *(15:22 Minutes)*

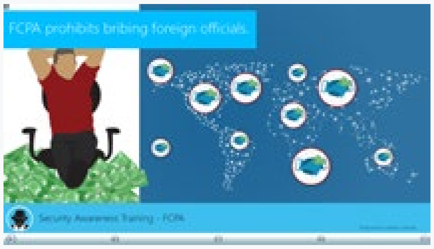
In this module, we review the new European Union General Data Protection Regulation (EU GDPR). It will define personal information per EU GDPR standards, provide common examples of personal data types and include a brief overview of the main goals and objectives of EU GDPR. Important EU GDPR terminology, EU GDPR requirements, best practices and repercussions of regulation violation are covered in detail.

Privacy violations may be accidental or intentional.

Security Awareness Training - Privacy and EU GDPR

FCPA *(9:34 Minutes)*

The Foreign Corrupt Practices Act (FCPA) monitors the international business community to prevent occurrence of bribes, kickbacks and other unacceptable business practices. This module defines the FCPA and outlines compliance needs, explores important definitions and provisions of the regulation, and suggests methods to help organizations avoid risks when conducting business with foreign officials.



FCPA prohibits bribing foreign officials.

Security Awareness Training - FCPA

FERPA *(7:14 Minutes)*

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. In this module, we identify who is impacted by FERPA, discuss the types of information that are protected by FERPA and detail what must be documented when a FERPA request is made.

Security Awareness Training - FERPA

GLBA *(6:25 Minutes)*

This module will define the Gramm-Leach-Bliley Act (GLBA), explain its purpose and detail the consequences of non-compliance. The three main sections of the GLBA -- Financial Privacy Rule, Safeguards Rule and Pretexting Provisions -- are covered in detail. It also defines nonpublic personal information in context of common working environments, and also reinforces the role of policy in maintaining personal data security.

GLBA includes Financial Privacy Rule, Safeguards Rule, and Pretexting Provisions
PRIVACY POLICY
Security Awareness Training - GLBA

SOX *(4:56 Minutes)*

This module covers The Sarbanes-Oxley Act of 2002 (SOX), a law enacted to combat major, large-scale corporate and accounting fraud. In this module, we'll review SOX mandates to enhance corporate responsibility, improve financial disclosures and combat corporate and accounting fraud. Fraud-prevention safeguards and other SOX mandates will also be discussed.

Red Flags Rule *(6:05 Minutes)*

The Red Flags Rule requires financial institutions and creditors to develop written programs, or an Identity Theft Prevention Program, to detect and avoid identity theft. This module will explain the program requirement, define key areas of the regulation and detail the four required steps of an Identity Theft Prevention Program: identifying red flags, detecting red flags, responding to red flags and updating the program.

Start with identifying the Red Flags relevant to your organization
!
Security Awareness Training - Red Flags Rule

Malware & Phishing Modules

Role-based customization available for all staff levels, industries and departments.

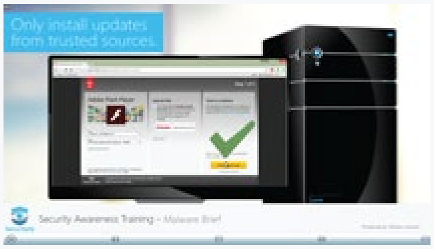
Malware *(17:01 Minutes)*

This interactive module defines malware in common terms and details the dangers it poses to organizations. Practical and applicable preventative actions are summarized in three anti-malware recommendations: avoiding suspicious downloads, attachments and other files, frequent/automated software patches and proper use of anti-virus software.

Drag and drop the viruses to items that can be infected.

Malware Brief *(3:37 Minutes)*

An abbreviated version of our core malware training, this module focuses on three key ways to prevent malware infections, details common sources of malware infections and discusses methods to help users avoid unsafe files.



Only install updates from trusted sources.

Malware for Executives *(7:23 Minutes)*

Executives are often targeted by hackers via malware, or malicious software. This module explains malware risks in detail and outlines steps executives can take to proactively keep their data secure. Suggested security policies and staff communication are also introduced in this module.

If an executive's computer gets infected with malware, the damage may be considerably larger.

Malware for Managers *(8:41 Minutes)*

Like executives, managers are often targeted by hackers due to their access to sensitive information. This module will help managers understand the risks of malware, teach them how to prevent installation and provide guidance on how managers can help their team understand -- and comply with -- internal security policies.

Managers need to be handle a wide array of incidents.

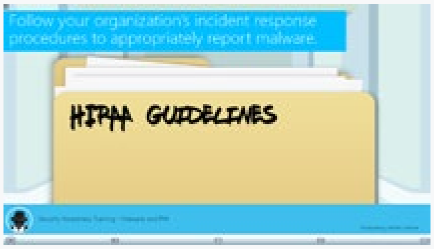
Malware for Financial Institutions *(8:04 Minutes)*

This interactive module defines malware in common terms and details the dangers it poses to financial organizations. Practical and applicable preventative actions are summarized in three anti-malware recommendations: avoiding suspicious files, frequent/automated software patches and proper use of anti-virus software. Banking Trojans are described as an example of malware specifically targeting financial information.

Managers need to be handle a wide array of incidents.
IT DEPARTMENT
ISSUE#112358-13A
MALWARE POLICY
INCIDENT REPORT #112358-13A
IT
Security Awareness Training - Malware For Managers

Malware & PHI *(9:36 Minutes)*

Hackers often target protected health information (PHI) using malware, or malicious software. Malware infections are considered a HIPAA security incident and can lead to severe penalties, as well as loss of information and patient trust. This module will teach healthcare professionals how to identify malware, and outline preventative actions organizations can take to avoid malware infections.


Follow your organization's incident response procedures to appropriately report malware.
HIPAA GUIDELINES
Security Awareness Training - Malware and PHI

Malware & PHI for Executives *(9:11 Minutes)*

This module explains how hackers target protected health information (PHI) using malware, or malicious software. Malware infections are considered a HIPAA security incident and can lead to severe penalties, as well as loss of information and patient trust. This training outlines steps healthcare executives can take to proactively keep PHI secure. Suggested security policies and staff communication strategies are also introduced in this module.

Managers need to be handle a wide array of incidents.
IT DEPARTMENT
ISSUE#112358-13A
MALWARE POLICY
INCIDENT REPORT #112358-13A
IT
Security Awareness Training - Malware For Managers

Malware & PHI for Managers *(10:25 Minutes)*

Hackers often target protected health information using malware, or malicious software. Malware infections are considered a HIPAA security incident and can lead to severe penalties, as well as loss of information and patient trust. This module will help healthcare managers understand the risks of malware, teach them how to prevent installation and provide guidance on how managers can help their team understand — and comply with — internal security policies.

Malware losses are real and very large.
Security Awareness Training - Malware and PHI for Managers

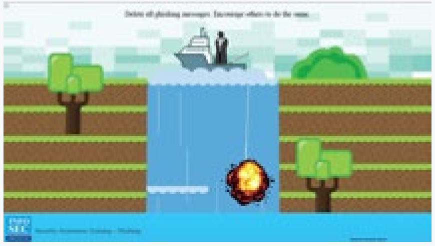
What is Phishing? *(1:46 Minutes)*

This brief phishing video details common phishing indicators and how they work, including how to spot malicious links and host names.

HACKERS FISH FOR VICTIMS USING INTERESTING MESSAGES AS BAIT
Security Awareness Training - What is Phishing?

Phishing *(20:50 Minutes)*

Phishing occurs when hackers use electronic messages (often email) to entice unsuspecting users to share personal information like passwords and credit card information. Our interactive phishing training outlines where phishing messages may appear, how to distinguish phishing from normal communications, and when and how to report phishing attacks.


Delete all phishing messages. Encourage others to do the same.
Security Awareness Training - Phishing

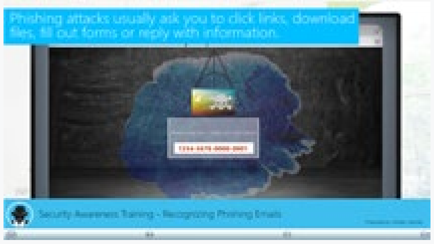
Phishing Brief *(3:06 Minutes)*

An abbreviated version of our core phishing training, this module will introduce learners to the concept of phishing, teach them how to quickly identify phishing messages and show them how to verify whether or not a message is legitimate.

Tricking people with access is often easier than hacking computers.
Security Awareness Training - Phishing In Brief

Recognizing Phishing Emails *(2:26 Minutes)*

This brief phishing video details common phishing indicators and how they work, including how to spot malicious links and host names.


Phishing attacks usually ask you to click links, download files, fill out forms or reply with information.
Security Awareness Training - Recognizing Phishing Emails

Phishing for Executives *(10:04 Minutes)*

When it comes to phishing, executives are one of the most targeted group of email users due to their levels of access and authority. This module explains the risks phishing poses to executives and organizations, and suggests ways executives can work with their security teams and staff to keep information secure.

Whaling goes after users with the highest level of access and authority.

Security Awareness Training - Phishing For Executives

Phishing for Managers *(11:02 Minutes)*

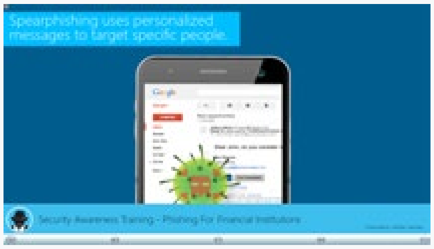
Managers are frequently targeted by phishing emails due to their level of data access. This module discusses phishing in detail and teaches managers how to detect phishing attempts. It also outlines how managers can work with their teams to protect their company from phishing attacks.

Managers and supervisors need to be able to recognize phishing threats.

Security Awareness Training - Phishing for Managers

Phishing for Financial Institutions *(10:23 Minutes)*

Phishing occurs when hackers use electronic messages (often email) to trick users into sharing personal information like passwords and credit card information. This interactive training explains how financial sector employees and customers are targeted by phishing attacks and teaches users how to distinguish phishing from normal communications. Topics include the importance of reporting phishing attempts, how to identify fake money transfer requests and how financial sector employees can protect customers by recognizing phishing attacks.



Spearphishing uses personalized messages to target specific people.

Security Awareness Training - Phishing For Financial Institutions

Business Email Compromise (BEC) *(1:14 Minutes)*

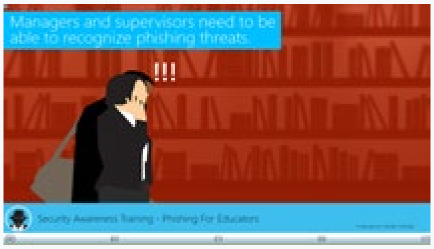
BEC scams occur when attackers impersonate company stakeholders (usually executives or vendors) and trick your employees into transfering money or sharing confidential information. This module explains what BEC is, and suggests defenses against this tactic, such as double checking money transfer requests.

It is important for executives to lead by example in following basic security best practices and complying with security policies.

Security Awareness Training - Business Email Compromise (BEC)

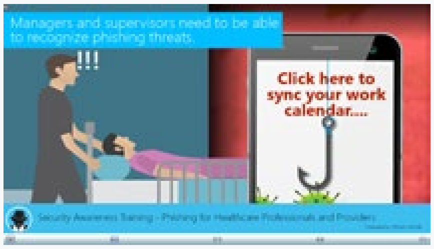
Phishing for Educators *(9:14 Minutes)*

Phishing occurs when hackers use electronic messages (often email) to trick users into sharing personal information like passwords and credit card information. This interactive training explains how education-sector employees and students are targeted by phishing attacks and teaches users how to distinguish phishing from normal communications. Topics include the importance of reporting phishing attempts, how to identify fake requests for student records and how educators can protect students and prevent identity theft by recognizing phishing attacks.


Managers and supervisors need to be able to recognize phishing threats.
!!!
Security Awareness Training - Phishing For Educators

Phishing for Healthcare Professionals & Providers *(11:07 Minutes)*

Healthcare professionals with direct or indirect access to protected health information are popular hacker targets. Protected health information is high-value data, and breaches from phishing attacks can lead to major fines. This module will define phishing, how to distinguish phishing from normal communications, and when and how to report phishing attacks.


Managers and supervisors need to be able to recognize phishing threats.
!!!
Click here to sync your work calendar....
Security Awareness Training - Phishing for Healthcare Professionals and Providers

Phishing for Healthcare Executives *(11:46 Minutes)*

When it comes to phishing, executives are one of the most targeted group of email users due to their levels of access and authority. This module explains the risks phishing poses to healthcare executives and organizations, and suggests ways executives can work with their security teams and staff to keep patient information secure.

Security Awareness Training - Phishing for Healthcare Executives

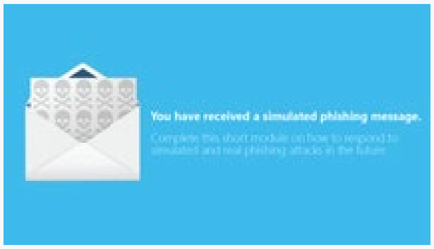
Phishing for Healthcare Managers *(13:39 Minutes)*

Healthcare professionals with direct or indirect access to protected health information (PHI) are popular hacker targets. Managers are frequently targeted by phishing emails due to their level of access to PHI. This module discusses phishing in detail and teaches healthcare managers how to detect phishing attempts. It also outlines how healthcare managers can work with their teams to protect their company from phishing attacks.

Managers and supervisors need to be able to recognize phishing threats.
Security Awareness Training - Phishing for Healthcare Managers

Reporting Phishing Emails *(1:10 Minutes)*

Our Reporting Phishing Emails module reviews the functionality of the PhishNotify button, which allows users to report suspicious emails to system administrators through Outlook, Office 365 and Gmail.



You have received a simulated phishing message.

Complete this short module on how to respond to simulated and real phishing attacks in the future.

Phishing Assessment (LinkedIn) *(30 Seconds)*

This advanced assessment module will test a learner's ability to recognize suspicious email elements through a realistic email mimicking LinkedIn communications.

The following email message contains several "Red Flags" - Or indications that it is a phishing email.

Examine the contents of the message, select the suspicious elements by clicking on them with your mouse.

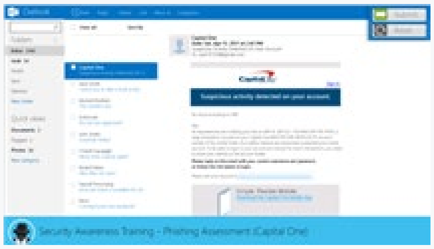
John Smith <BSmith@ea[illegible]ail.com

When you have identified all of the indicators of phishing please click the **Submit** button.

Submit
Security Awareness Training - Phishing Assessment (LinkedIn)

Phishing Assessment (Capital One) *(30 Seconds)*

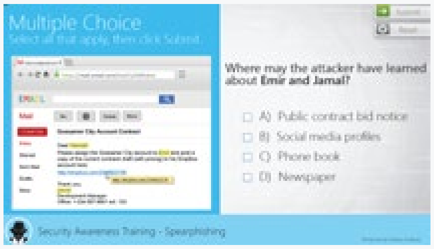
This assessment module will test a learner's ability to recognize suspicious email elements through a realistic email mimicking Capital One communications.



Outlook
Capital One
Suspicious activity detected on your account
Security Awareness Training - Phishing Assessment (Capital One)

Spearphishing *(2:40 Minutes)*

Spearphishing occurs when phishing messages are tailored for targeted individuals. This interactive module will help teams identify and avoid spearphishing attempts.



Multiple Choice

Select all that apply, then click Submit.

Where may the attacker have learned about **Emir and Jamal?**

- □ A) Public contract bid notice
- □ B) Social media profiles
- □ C) Phone book
- □ D) Newspaper

Ransomware *(4:38 Minutes)*

Ransomware is malware, or malicious software, that holds technology for ransom. This modules will show learners how ransomware works, what do if an infection occurs and how to avoid future infections.

Ransomware & HIPAA *(6:20 Minutes)*

This short module will teach learners the risks of ransomware in the healthcare industry, including whether a ransomware infection is considered a HIPAA data breach.

If ransomware strikes, isolate the machine, get help and restore from backups
Security Awareness Training - Ransomware and HIPAA

Antivirus *(0:47 Minutes)*

In less than 60 seconds, this video details the threats antivirus software can and cannot mitigate.

Use antivirus on devices that support it.
ANTIVIRUS
Security Awareness Training - Antivirus

Web-Application Based Threat Modules

Role-based customization available for all staff levels, industries and departments.

Safe Browsing *(10:58 Minutes)*

Our interactive Safe Browsing module shows learners how hackers can launch attacks from unsafe websites and outlines best practices for safe browsing. Topics include use of HTTPS (using SSL or TLS), unsafe links, web pop-ups, browser alerts, plugins and downloads. Lessons from our Phishing and Malware modules are also reinforced for increased retention.

Be careful of hostnames containing numbers.

https://16.32.134.217 or http://FE80:0202:B3FF:FE1E:8329

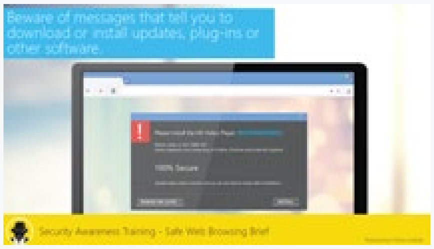
https://www.yahoo23.com or http://white62ho

https://www.m1croSof]

Security Awareness Training - Safe Web Browsing

Safe Web Browsing Brief *(5:03 Minutes)*

Our interactive Safe Browsing module shows learners how hackers can launch attacks from unsafe websites and outlines best practices for safe browsing. Topics include use of HTTPS (using SSL or TLS), unsafe links, web pop-ups, browser alerts, plugins and downloads. Lessons from our Phishing and Malware modules are also reinforced for increased retention.



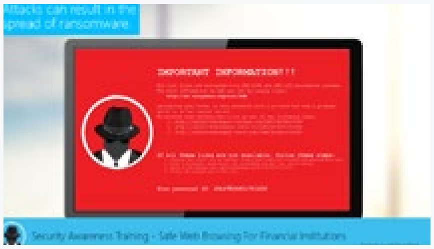
Beware of messages that tell you to download or install updates, plug-ins or other software.

100% Secure

Security Awareness Training - Safe Web Browsing Brief

Safe Web Browsing for Financial Institutions *(12:15 Minutes)*

Our interactive Safe Browsing module shows learners how hackers can launch attacks from unsafe websites and outlines best practices for safe browsing. Topics include use of HTTPS (using SSL or TLS), unsafe links, web pop-ups, browser alerts, plugins and downloads. Lessons from our Phishing and Malware modules are also reinforced for increased retention.



Attacks can result in the spread of ransomware

IMPORTANT INFORMATION!!!

Security Awareness Training - Safe Web Browsing For Financial Institutions

Safe Web Browsing for Educators *(12:18 Minutes)*

Our interactive Safe Browsing module shows learners how hackers can launch attacks from unsafe websites and outlines best practices for safe browsing. Topics include use of HTTPS (using SSL or TLS), unsafe links, web pop-ups, browser alerts, plugins and downloads. Lessons from our Phishing and Malware modules are also reinforced for increased retention.

Take your time installing software.

Security Awareness Training - Safe Web Browsing For Educators

Safe Browsing for Executives *(11:32 Minutes)*

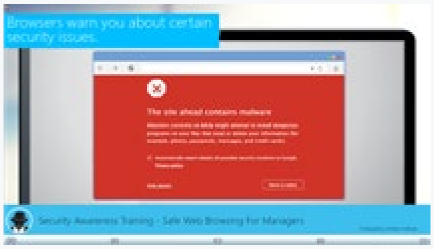
As prime cybercriminal targets, it's critical for executives to follow safe browsing best practices. The Safe Browsing for Executives module will explain safe browsing best practices for individuals and organizations, and provide guidance on how executives can work with IT and managers to implement and enforce safe-browsing policies.

It is crucial for executive managers to follow safe browsing best practices.

Security Awareness Training - Safe Web Browsing For Executives

Safe Browsing for Managers *(11:47 Minutes)*

This module shows managers how hackers launch attacks from unsafe websites and reinforces the need for managerial reinforcement of internal safe-browsing policies. Topics include use of HTTPS (using SSL or TLS), unsafe links, web pop-ups, browser alerts, plugins and downloads.



Browsers warn you about certain security issues.

The site ahead contains malware

Security Awareness Training - Safe Web Browsing For Managers

Safe Browsing for Healthcare Professionals & Providers *(12:33 Minutes)*

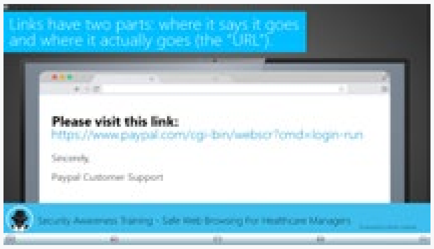
Healthcare professionals must take extra care to browse the web safely and avoid exposure of protected health information (PHI). This module will define safe browsing and show healthcare professionals how PHI can be compromised through malicious plugins and downloads.

Beware of messages that tell you to download or install updates, plug-ins or other software.

IMPORTANT INFORMATION!!!

Safe Web Browsing for Healthcare Managers *(12:40 Minutes)*

Healthcare professionals must take extra care to browse the web safely and avoid exposure of protected health information (PHI). This module shows healthcare managers how PHI can be compromised through malicious plugins and downloads, and reinforces the need for managerial reinforcement of internal safe-browsing policies. Topics include use of HTTPS (using SSL or TLS), unsafe links, web pop-ups, browser alerts, plugins and downloads.



Links have two parts: where it says it goes and where it actually goes (the "URL").

Please visit this link:
https://www.paypal.com/cgi-bin/webscr?cmd=login-run

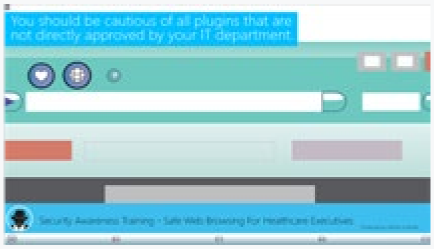
Sincerely,

Paypal Customer Support

Security Awareness Training - Safe Web Browsing For Healthcare Managers

Safe Web Browsing for Healthcare Executives *(12:58 Minutes)*

As prime cybercriminal targets, it's critical healthcare executives follow safe browsing best practices.The Safe Browsing for Healthcare Executives module will explain safe browsing best practices for individuals and organizations, and provide guidance on how executives can work with IT and managers to implement and enforce safe-browsing policies and avoid exposure of protected health information.

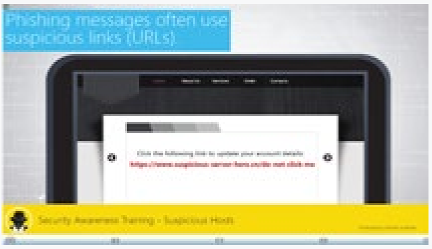


You should be cautious of all plugins that are not directly approved by your IT department.

Security Awareness Training - Safe Web Browsing for Healthcare Executives

Suspicious Hosts *(3:50 Minutes)*

Suspicious hosts are known malicious or potentially unsafe IP addresses or hostnames. This module will outline how safe browsing can protect Internet users from malicious attacks from suspicious hosts.



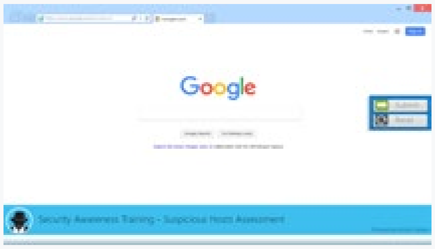
Phishing messages often use suspicious links (URLs)

Click the following link to update your account details:
https://www.suspicious-server-here.co/do-not-click-me

Security Awareness Training - Suspicious Hosts

Suspicious Host Assessment (Google) *(30 Seconds)*

This interactive module will test learners' abilities to recognize suspicious hosts in a realistic website simulation.



Security Awareness Training - Suspicious Hosts Assessment

Mobile Security Modules

Role-based customization available for all staff levels, industries and departments.

Mobile Security *(10:31 Minutes)*

This module identifies security risks resulting from business-based mobile device use in public places and on public networks. It provides suggested mobile device best practices like screen locks, device encryption and Wi-Fi validation.

Never just insert a "found" drive or CD – it can infect your computer!

Mobile Security for Executives *(6:05 Minutes)*

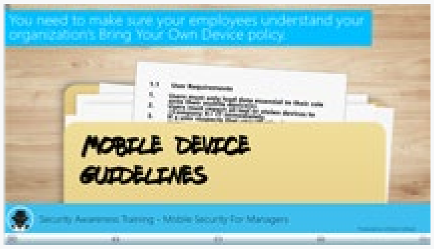
Executives have advanced permissions and access to large amounts of sensitive data, making them prime targets for hacking attempts. In this module, we review the risks of conducting business on mobile devices and public networks, and share best practices for working remotely at home and abroad. Suggested organizational-level mobile device policies are also introduced.

Mobile devices are used in hostile environments.

Security Awareness Training - Mobile Security For Executives

Mobile Security for Managers *(7:03 Minutes)*

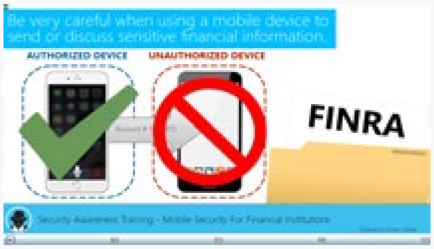
It's essential that managers understand and support mobile device security policies at the office. This module will explain the risks of mobile devices and public networks in detail, and provide guidance on how managers can work with their teams to keep sensitive data secure.



You need to make sure your employees understand your organization's Bring Your Own Device policy.

Mobile Security for Financial Institutions *(6:31 Minutes)*

This module identifies the security risks financial institutions face from business-based mobile device use. It provides suggested mobile device best practices like using screen locks, device encryption and Wi-Fi validation. The module explains other threats facing the industry, including malicious applications designed to attack financial accounts and possible FINRA violations from sharing business information via mobile communications.



Be very careful when using a mobile device to send or discuss sensitive financial information.

AUTHORIZED DEVICE
UNAUTHORIZED DEVICE
FINRA
Security Awareness Training - Mobile Security For Financial Institutions

Mobile Security for Healthcare Professionals *(7:22 Minutes)*

Mobile devices like smartphones have become an integral part in the daily tasks of healthcare professionals. This security awareness module covers best practices for ensuring HIPAA compliance when using mobile devices to store or access protected health information. It also suggests tips to keeping mobile devices secure, such as using locks, encryption, antivirus and frequent system updates.

Mobile devices introduce serious privacy and security risks.
Health Care Tools 1.0

Mobile Security for Educators *(6:00 Minutes)*

This module identifies the security risks educational institutions face from business-based mobile device use. It provides suggested mobile device best practices like using screen locks, device encryption and Wi-Fi validation. The module explains the importance of protecting devices used to access student data and considerations when using third-party educational applications.

Be careful when supplying student information to third party apps.
IT APPROVED MOBILE APPS
PRIVACY OFFICER
Security Awareness Training - Mobile Security For Educators

Mobile Security for Healthcare Executives *(6:49 Minutes)*

With advanced permissions and access to large amounts of sensitive data — including PHI — executives are prime targets for hacking attempts. In this module, we review the risks of conducting business on mobile devices and public networks, and share best practices for working remotely at home and abroad. Suggested organizational-level mobile device policies are also introduced.

To keep phone and devices safe, use antivirus, update them, and be careful with wireless options.
Can this app access telephony?
Security Awareness Training - Mobile Security For Healthcare Executives

Mobile Security for Healthcare Managers *(6:49 Minutes)*

Mobile devices like smartphones are an integral tool used in the daily tasks of healthcare professionals. It's essential that managers understand and support mobile device security policies at the office to keep data secure. This security awareness module covers best practices for ensuring HIPAA compliance when using mobile devices to store or access protected health information. It also suggests tips to keeping mobile devices secure, such as using locks, encryption, antivirus and frequent system updates.

Mobile devices are increasingly used alongside workplace computers.
Security Awareness Training - Mobile Security For Healthcare Managers

Mobile Wi-Fi Security *(2:42 Minutes)*

Our Mobile Wi-Fi Security module explains how to safely use wireless devices when operating on Wi-Fi connections.

Limit which networks your device remembers.

Securing Mobile Devices *(2:20 Minutes)*

Mobile devices are often used for both personal and business applications. This demands a different approach to information security than traditional workplace solutions. This module will inform learners on the differences between mobile devices and traditional desktop computers in the context of information security, and teach learners how to use mobile devices safely.

Multiple Choice

Select the most secure phone

Network Security Modules

Role-based customization available for all staff levels, industries and departments.

Public Networks and Computers *(4:14 Minutes)*

Public networks are a convenient connectivity option, but pose a number of security challenges. This training module will teach learners how limit security risks while using public networks and computers.

Public wireless and cellular networks are convenient but often shared with hackers.

Security Awareness Training - Public Networks and Computers

Securing Home Networks and Devices *(3:29 Minutes)*

Protecting home computers and networks can help keep company networks secure, especially those with remote or mobile workforces. This interactive module shows learners how to implement many of the same protections at home that IT staff use at the office.

To keep your home network safe, pick strong passwords, disable remote access, and update your router.

Security Awareness Training - Securing Home Networks and Devices

Working Remotely *(12:23 Minutes)*

Designed specifically for remote workers, this interactive module details networking essentials and best security practices to help keep remote personnel secure. Learners will gain deeper understanding of home networks and the devices and risks that come with them, and learn why use of public networks and devices should be avoided when possible.

Wireless traffic can be intercepted unless it is protected.

Security Awareness Training - Working Remotely

Working Remotely for Executives *(10:24 Minutes)*

Executives often work remotely from home or when traveling. This module details best practices for working remotely on secure networks, including Wi-Fi safety and VPN connections. It also provides guidance on what executives can do to ensure they and all other employees are protecting their devices, data and access.

Use SSL (TLS or HTTPS) or VPN to encrypt communications over public networks.

Security Awareness Training - Working Remotely For Executives

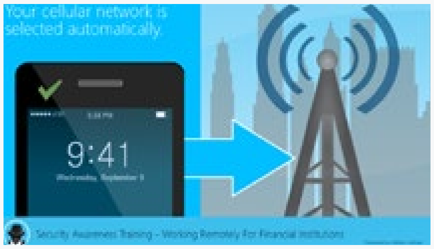
Working Remotely for Managers *(10:47 Minutes)*

More and more frequently, managers and their teams conduct work from remote locations. This module details best practices for working remotely on secure networks, including Wi-Fi safety and VPN connections, and reinforces the need for managerial support of remote security policies. It also provides guidance on what managers can do to ensure their teams are protecting their devices, data and access.

Your cellular network is selected automatically.

Working Remotely for Financial Institutions *(11:10 Minutes)*

Designed specifically for financial sector employees working remotely, this interactive module details networking essentials and security best practices to help keep remote personnel secure. Learners will gain deeper understanding of home networks and the devices and risks that come with them, and learn why use of public networks and devices to access sensitive financial information should be avoided when possible. Use of secure communication methods to ensure confidentiality and integrity of transactions is also covered.

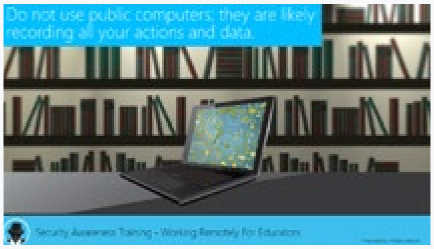


Your cellular network is selected automatically.

9:41
Wednesday, September 9
Security Awareness Training - Working Remotely For Financial Institutions

Working Remotely for Educators *(10:39 Minutes)*

Designed specifically for education-sector employees working remotely, this interactive module details networking essentials and best security practices to help keep remote personnel secure. Learners will gain deeper understanding of home networks and the devices and risks that come with them, and learn why use of public networks and devices to access sensitive student information should be avoided when possible. Secure methods for accessing student data remotely are discussed.

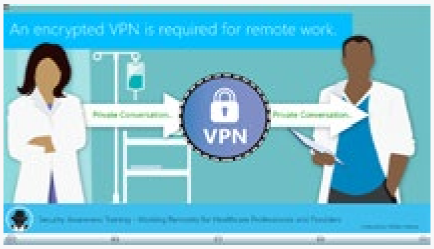


Do not use public computers; they are likely recording all your actions and data.

Security Awareness Training - Working Remotely For Educators

Working Remotely for Healthcare Pros & Providers *(10:44 Minutes)*

Healthcare professionals require access to valuable protected health information, making them a target for hacking attempts. This module will outline HIPAA requirements for working remotely, such as using encrypted VPNs and securing personal devices. Other topics include Wi-Fi security, public network risks and at-home network security.



An encrypted VPN is required for remote work.

Private Conversation...
VPN
Private Conversation...
Security Awareness Training - Working Remotely for Healthcare Professionals and Providers

Working Remotely for Healthcare Executives *(12:01 Minutes)*

Healthcare executives have access to valuable protected health information. They often work remotely from home or when traveling, making them a target for hacking attempts. This module details best practices for working remotely on secure networks, including Wi-Fi safety and VPN connections. It also provides guidance on what healthcare executives can do to ensure they and all other employees are protecting their devices, data and access.

You give up many protections by working remotely.

Security Awareness Training - Working Remotely for Healthcare Executives

Working Remotely for Healthcare Managers *(11:49 Minutes)*

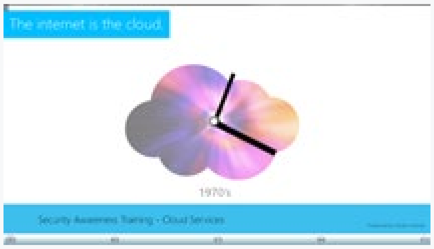
Healthcare managers have access to valuable protected health information. More and more frequently, these managers and their teams conduct work from remote locations. This module details best practices for working remotely on secure networks, including Wi-Fi safety and VPN connections. It also provides guidance on what healthcare managers can do to ensure they and all other employees are protecting their devices, data and access.

Always check the SSID name and "password icon" before connecting.

Security Awareness Training - Working Remotely for Healthcare Managers

Cloud Services *(6:53 Minutes)*

Cloud services include any service available via the Internet through a third-party's server. This module will define the cloud and different types of cloud services available, and explain the benefits and risks of cloud-based services. Tips for using cloud services in a safe and responsible way are included in the module.



The internet is the cloud.

1970's

Security Awareness Training - Cloud Services

Advanced Persistent Threat (APT) *(7:22 Minutes)*

An advanced persistent threat (APT) occurs when an unauthorized user gains network access and remains undetected for long periods of time. This module explains how to recognize APTs, APT risks and common attack methods. A real APT attack is used to demonstrate the danger and lifecycle of typical APT attacks. Tips on APT attack prevention are also included in the module.

ADVANCED
PERSISTENT
THREAT

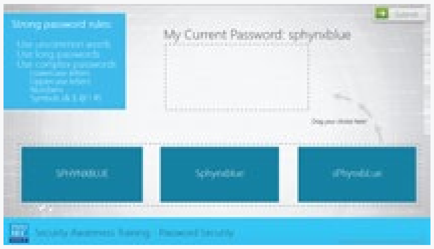
Security Awareness Training - APT

Password Security Modules

Role-based customization available for all staff levels, industries and departments.

Password Security *(21:16 Minutes)*

Our interactive Password Security module shows learners how to create complex, but easy-to-remember, passwords following best practices for password creation. We'll explain how passwords may be stolen, and share real-world scenarios where weak or shared passwords compromise security.

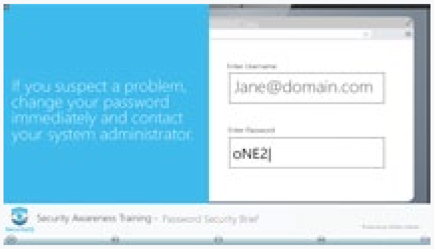


Strong password rules:
- Use uncommon words
- Use long passwords
- Use complex passwords
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Symbols

My Current Password: sphynxblue

Password Security Brief *(4:37 Minutes)*

An abbreviated version of our core password security training, this module will summarize the best practices associated with creating and managing strong passwords, how to safely store passwords and what to do if you suspect that a password has been compromised.



If you suspect a problem, change your password immediately and contact your system administrator.

Enter Username: Jane@domain.com

Enter Password: oNE2|

Creating Strong Passwords *(0:46 Minutes)*

This short video details the process of choosing secure, robust passphrases in under one minute. Topics include the importance of using uncommon words and long passphrases.

A strong password is hard to guess.

Secure Password Storage *(1:05 Minutes)*

This short video introduces methods employees can use to store passwords securely. Topics include physical security and password storage applications.

Protect a written password like cash.

Password Security for Executives *(10:39 Minutes)*

Passwords of executive-level staff are a high-value target for cyber criminals. This module will teach executives how to create strong passwords and keep them safe, and show executives how they can personally support secure password management policies and habits within their companies.

Hello Jane

Would you like to send the email titled "You're All FIRED" to your team?

Yes/No

Security Awareness Training - Password Security For Executives

Password Security for Managers *(11:50 Minutes)*

Managers have a responsibility to not only set secure passwords for themselves, but also to ensure their teams follow best practices in password security. This module will show managers how to pick strong passwords and keep them safe, how to securely set passwords for employees and how to help employees with password security related issues.

Protect a written password like cash

Accessing folder: EXECUTIVE PAYROLL at 'REMOTESERVER1'

Security Awareness Training - Password Security For Managers

Password Security for Healthcare Pros & Providers *(9:25 Minutes)*

Based on password-related HIPAA requirements, this module stresses the importance of following internal policies regarding access to protected health information. It will show healthcare professionals how to create complex, effective passwords, and share real-world scenarios where weak or shared passwords compromise security.

Use only approved authentication methods

Password Security for Healthcare Executives *(10:46 Minutes)*

Passwords belonging to executive-level staff are a high-value target for cybercriminals, especially if these passwords may provide access to protected health information. This module will teach healthcare executives how to create strong passwords and keep them safe, and show executives how they can personally support secure password management policies and habits within their companies.

Never share passwords that protect PHI

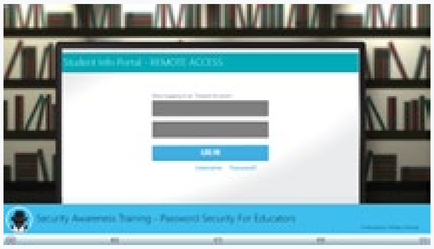
Patient Info Portal

SharedAccount

Security Awareness Training - Password Security for Healthcare Executives

Password Security for Educators *(10:01 Minutes)*

Our interactive Password Security module stresses the importance of following internal policies regarding access to sensitive student information. It will show education professionals how to create strong passwords, and share real-world scenarios where weak or improperly shared passwords compromise security. It also stresses the importance of unique credentials for accessing student records.

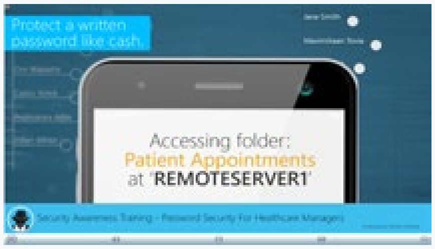


Password Security for Financial Institutions *(9:32 Minutes)*

Our interactive Password Security module stresses the importance of following internal policies regarding access to sensitive financial information. It will show financial industry professionals how to create strong passwords, and share real-world scenarios where weak or improperly shared passwords compromise security.

Password Security for Healthcare Managers *(10:32 Minutes)*

Managers have a responsibility to not only set secure passwords for themselves, but also to ensure their teams follow best practices in password security. Based on password-related HIPAA requirements, this module stresses the importance of following internal policies regarding access to protected health information. It will show healthcare managers how to pick strong passwords and keep them safe, how to securely set passwords for employees and how to help employees with password security related challenges.



CJIS Policy: Handling CJI *(9:02 Minutes)*

This module defines criminal justice information (CJI), the protocols required to access and handle CJI and the consequences of noncompliance.

CHRI is arrest-based data and any derivative information from that record.

CJIS Security Policy *(5:26 Minutes)*

This module provides a detailed explanation of criminal justice information security (CJIS) policy requirements, outlines who must comply with CJIS policy and details how to respond to incidents involving criminal justice information.

Any entity with access to CJI must comply.
Security Awareness Training - CJIS Security Policy

CJIS Policy: Physical Security *(9:25 Minutes)*

This module covers the necessary defenses against unauthorized access to your facility and any paper copies of criminal justice information in your possession.

Security Awareness Training - CJIS Policy: Physical Security

CJIS Policy: Media Protection *(7:52 Minutes)*

Any physical media containing criminal justice information must be protected. This module outlines data-handling best practices, such as avoiding malware, applying encryption and proper disposal of physical media.

CJIS Policy: Dissemination & Destruction *(7:05 Minutes)*

Criminal justice information (CJI) must be collected, stored, accessed and disposed of securely. This module outlines how to properly dispose of CJI, how to locate and remove CJI securely, when CJI should be destroyed and best practices for destroying CJI.

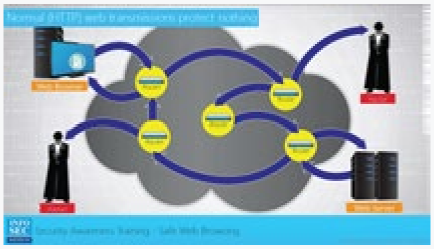
Data destruction must be permanent and irreversible.
Security Awareness Training - CJIS Policy: Dissemination and Destruction

Physical Security & Hardware Modules

Role-based customization available for all staff levels, industries and departments.

Physical Security *(13:00 Minutes)*

Physical security helps prevent losses of information and technology in the physical environment. This interactive module identifies physical security vulnerabilities, like printers and trash cans, and the risks employees face when technology is left unattended in publicly accessible areas. Prevention tactics to combat each type of risk is also discussed.



Normal (HTTP) web transmissions protect nothing

Security Awareness Training - Safe Web Browsing

Physical Security Brief *(6:06 Minutes)*

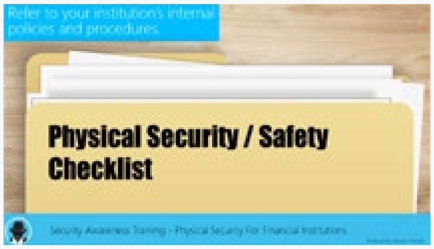
An abbreviated version of our physical security training, this module provides basic understanding of how to avoid theft and misuse of printed materials and unattended technology.

Printouts are not subject to virtual controls.

Security Awareness Training - Physical Security Brief

Physical Security for Financial Institutions *(9:33 Minutes)*

This module will review best practices for physical security as it relates to protecting printed financial and personal information, including facility access, device storage, physical record management and electronic record transmission.



Refer to your institution's internal policies and procedures.

Physical Security / Safety Checklist

Security Awareness Training - Physical Security For Financial Institutions

Physical Security and Student Records *(9:32 Minutes)*

This module will review best practices for physical security as it relates to protecting printed student educational and personal information, including facility access, device storage, physical record management and electronic record transmission.

Unattended technology is at risk of theft or misuse.

Security Awareness Training - Physical Security And Student Records

Physical Security for Executives *(10:17 Minutes)*

Based on password-related HIPAA requirements, this module stresses the importance of following internal policies regarding access to protected health information. It will show healthcare professionals how to create complex, effective passwords, and share real-world scenarios where weak or shared passwords compromise security.

Unattended technology is at risk of theft or misuse.
Security Awareness Training - Physical Security For Executives

Physical Security for Managers *(9:28 Minutes)*

Managers have a responsibility to teach and reinforce the importance of physical security in the office. This module will explain the need for physical security to keep data secure, and teach managers how to avoid theft and misuse of printed materials and unattended technology.

Printouts are not subject to virtual controls.
Security Awareness Training - Physical Security For Managers

Physical Security & PHI *(00:00 Minutes)*

HIPAA includes specific requirements for physical safeguards that every organization should have in place to secure protected health information (PHI). This module will review best practices for physical security as it relates to HIPAA compliance, including facility access, device storage, physical record management and electronic record transmission.

Printouts are not subject to virtual controls.
Security Awareness Training - Physical Security Brief

Physical Security & PHI for Healthcare Executives *(11:42 Minutes)*

HIPAA outlines specific physical security requirements that every organization should have in place to secure protected health information. Executives often carry physical documents and hardware containing highly sensitive information. This module will review best practices for physical security as it relates to HIPAA compliance, including facility access, device storage, physical record management and electronic record transmission.

Printouts are not subject to virtual controls.
Security Awareness Training - Physical Security and PHI for Executives

Physical Security & PHI for Healthcare Managers *(12:14 Minutes)*

HIPAA requires specific physical safeguards to secure protected health information at healthcare facilities. Managers in healthcare have a responsibility to teach and reinforce the importance of physical security in the office.This module will review best practices for physical security as it relates to HIPAA compliance, including facility access, device storage, physical record management and electronic record transmission.

Follow all policies your organization has in place for using removable media and handling PHI.

Security Awareness Training - Physical Security For Healthcare Managers

Removable Media *(10:47 Minutes)*

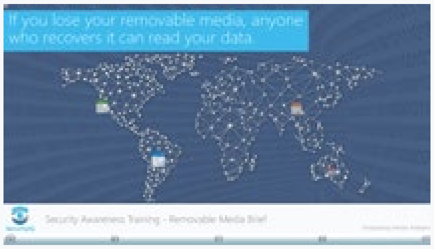
Removable media includes USB drives, CDs and personal devices such as phones, cameras and tablets. This interactive module covers two key areas of focus: safe use of removable media for legitimate purposes, and types of attacks hackers launch from “lost” removable media.

Removable media offers a convenient way to share file with other people.

Security Awareness Training - Removable Media

Removable Media Brief *(3:20 Minutes)*

An abbreviated version of our core removal media training, this summary course gives learners a basic understanding of the risks associated with removable media and how to avoid infection from these devices.


If you lose your removable media, anyone who recovers it can read your data.

Security Awareness Training - Removable Media Brief

Removable Media for Financial Institutions *(7:30 Minutes)*

This interactive module covers security risks to financial institutions posed by removable media. It focuses on the following key areas: safe use of removable media for legitimate purposes, types of attacks hackers launch from “lost” removable media and risks of financial data breaches from lost or stolen media.

major data breach.

Security Awareness Training - Removable Media For Financial Institutions

Removable Media for Educators *(7:42 Minutes)*

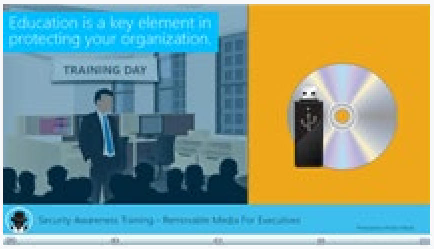
This interactive module covers security risks to educational institutions posed by removable media. It focuses on the following key areas: safe use of removable media for legitimate purposes, types of attacks hackers launch from "lost" removable media, and risks of student data breaches from lost or stolen media.

Always run antivirus software. It can also scan removable media.

Security Awareness Training - Removable Media For Educators

Removable Media for Executives *(7:20 Minutes)*

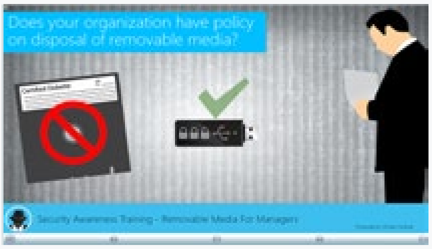
Executives must lead and support policies to prevent infections from removable media. This interactive module covers three key areas of focus: safe use of removable media for legitimate purposes, types of attacks hackers launch from "lost" removable media and best practices for preventing infection from a malicious device.


Education is a key element in protecting your organization.

Security Awareness Training - Removable Media For Executives

Removable Media for Managers *(8:21 Minutes)*

Managers interact the most with the general workforce, making it their responsibility to understand -- and enforce -- removable media policies. This module will explain the risks associated with removable media like USB drives, and provide guidance on how managers can help employees use removable media securely.


Does your organization have policy on disposal of removable media?

Security Awareness Training - Removable Media For Managers

Removable Media & PHI *(8:26 Minutes)*

Medical devices are often networked or require USB connection for data transfer, making them vulnerable to malware. This module details best practices healthcare professionals can follow to safeguard protected health information and avoid infection from removable media.

or using removable media and handling PHI.

Security Awareness Training - Removable Media and PHI

Removable Media & PHI for Healthcare Managers *(9:59 Minutes)*

Medical devices are often networked or require USB connection for data transfer, making them vulnerable to malware. Managers interact the most with the general workforce, making it their responsibility to understand — and enforce — removable media policies. This module details best practices healthcare managers can follow to safeguard protected health information and avoid infection from removable media.

Education is a key element in protecting your organization.
TRAINING DAY
Security Awareness Training - Removable Media and PHI for Managers

Removable Media & PHI for Executives *(9:13 Minutes)*

Medical devices are often networked or require USB connection for data transfer, making them vulnerable to malware. Healthcare executives must lead and support policies to prevent infections from removable media and ensure HIPAA compliance. This module details best practices healthcare executives can implement across their organizations to safeguard protected health information and avoid infection from removable media.

Education is a key element in protecting your organization.
TRAINING DAY
Security Awareness Training - Removable Media and PHI for Managers

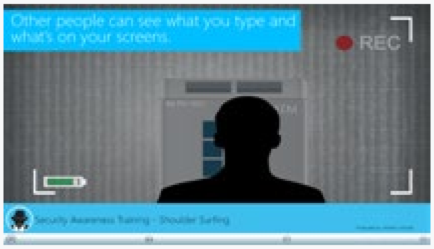
Tailgating *(1:42 Minutes)*

In less than two minutes, this video explains the risks of tailgating, or when hackers gain physical access to restricted areas. It also details physical security best practices for your office or campus.

Trespassers often follow authorized people into buildings, rooms, and other secured areas.
Security Awareness Training - Tailgating

Shoulder Surfing *(1:16 Minutes)*

Hackers use shoulder surfing to steal sensitive information directly from devices in-person or through cameras. In less than two minutes, this video explains what shoulder surfing is and emphasizes the importance of situational awareness when entering sensitive information in public settings.


Other people can see what you type and what's on your screens.
REC
Security Awareness Training - Shoulder Surfing

Updates & Patches *(1:39 Minutes)*

One of the simplest and easiest ways to protect yourself from attacks is to keep your software up to date. This module covers the importance of regular patches and updates, and also details how to avoid malicious updates from untrusted sources.

Apply regular updates, or "patches," to your existing software
Version: 1.0
Version: 1.2
Security Awareness Training - Updates and Patches

Protecting Mobile Devices *(1:17 Minutes)*

In a little over a minute, this video covers the steps you can take to protect your device from prying eyes and theft. Topics include screen locks, encryption and frequent software and firmware updates.

Social Engineering Modules

Role-based customization available for all staff levels, industries and departments.

Social Engineering *(12:54 Minutes)*

Social engineering occurs when a hacker uses two-way forms of communication, including phones and messaging, to trick users into sharing personal or confidential information. Our Social Engineering module teaches a three-step method to add clarity to a confusing conversation, challenge the other person's identity and verify suspicious requests.

Social engineering requires contact and trust.
Security Awareness Training - Social Engineering

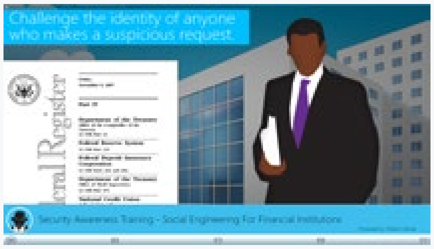
Social Engineering Brief *(4:11 Minutes)*

An abbreviated version of our core social engineering training, this module walks learners through the key components of social engineering and how to recognize and respond to suspicious requests.

You can identify social engineering attacks as they occur.
(3) INDICATORS:
Security Awareness Training - Social Engineering Brief

Social Engineering for Financial Institutions *(7:21 Minutes)*

Social engineering occurs when hackers use two-way forms of communication, including calls and messages, to trick users into sharing personal or confidential information. This social engineering module teaches a three-step method to add clarity to a confusing conversation, challenge the other person's identity and verify suspicious requests. Topics include fake money transfer requests, pretexting (as a social engineering technique as well as a practice prohibited by GLBA provisions) and identity theft prevention prescribed by the Red Flags Rule.


Challenge the identity of anyone who makes a suspicious request.
Federal Register
Security Awareness Training - Social Engineering For Financial Institutions

Social Engineering for Educators *(7:03 Minutes)*

Social engineering occurs when a hacker uses two-way forms of communication, including phones and messaging, to trick users into sharing personal or confidential information. Our Social Engineering module teaches a three-step method to add clarity to a confusing conversation, challenge the other person's identity and verify suspicious requests.

I'm going to need to verify some thing, before we can move forward here. It should only take a second.
Security Awareness Training - Social Engineering For Educators

Social Engineering for Healthcare Pros & Providers *(9:45 Minutes)*

Due to the high value of protected health information (PHI), healthcare professionals are frequently targeted by hackers via social engineering. This module will explain social engineering techniques in detail, and review HIPAA requirements regarding external requests for PHI.

As a healthcare professional or provider you should be able to handle high pressure situations.
Security Awareness Training - Social Engineering for Healthcare Professionals and Providers

Social Engineering for Healthcare Managers *(7:33 Minutes)*

Due to the high value of protected health information (PHI), healthcare professionals are frequently targeted by hackers via social engineering. Managers are often impersonated in spearphishing attempts, making the ability to identify social engineering attacks an essential managerial skill. This module will explain the various social engineering methods hackers use, review HIPAA requirements regarding external requests for PHI, and teach managers how to work with staff to prevent PHI breaches and leaks.

As a healthcare professional or provider you should be able to handle high pressure situations.
Security Awareness Training - Social Engineering for Healthcare Managers

Avoiding Cybersecurity Risks for Executives *(9:45 Minutes)*

Malicious hackers often target top-level managers for quicker, larger and more effective attacks. This security awareness module explains why top-level managers are targeted, details common attack methods used against executives and offers recommendations for avoiding security risks.

Executives are targeted because they have immediate access to resources and are more exposed.
Security Awareness Training - Avoiding Cybersecurity Risks for Executives

Social Media *(6:14 Minutes)*

Social media has become an integral part of everyday life for individuals and businesses. In many cases, it is the primary method used to communicate with friends, family and customers. This module explains common security risks related to the use of social media in business, and ways that learners can protect themselves and their company from social media threats.

Notification from Acme Corp
Security Awareness Training - Social Media

Social Media for Financial Institutions

(6:31 Minutes)

Social media has become an integral part of everyday life for individuals and businesses. In many cases, it is the primary method used to communicate with friends, family and customers. This module explains common security risks financial sector employees face when using social media at work, and ways that learners can protect themselves and their company from social media threats. FINRA regulations applicable to business communications via social media are also explained.

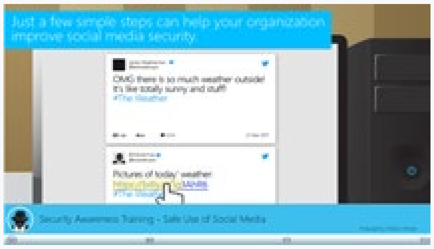
As a healthcare professional or provider you should be able to handle high pressure situations.

Security Awareness Training - Social Engineering for Healthcare Professionals and Providers

Safe Use of Social Media

(1:35 Minutes)

Social media can be a useful tool, but appropriate care should be taken when sharing personal information on social networks and clicking links shared by others. This short video covers the precautions you should take when making public posts and provides guidance on how to spot harmful links.



Just a few simple steps can help your organization improve social media security.

OMG there is so much weather outside! It's like totally sunny and stuff! #The Weather

Pictures of today' weather

Security Awareness Training - Safe Use of Social Media

Social Engineering Defenses

(1:31 Minutes)

This brief video shows you how to recognize and prevent social engineering attacks. Three key defenses are outlined in the video: challenge requester's identity, verify requests with supervisors and slow down the interaction.

(3) DEFENSES:

1. Challenge the requester's identity
2. Verify the suspicious request with your supervisor
3. Slow down or pause the interaction

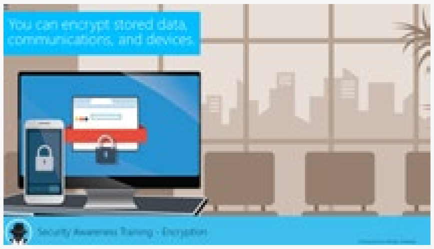
Security Awareness Training - Social Engineering Defenses

Internal Control Modules

Role-based customization available for all staff levels, industries and departments.

Encryption *(6:14 Minutes)*

This module explains the concept of encryption in common terms. It details the encryption process and types of assets that can be encrypted, and reinforces the importance of following encryption-related policies to protect sensitive information.



You can encrypt stored data, communications, and devices.

Data Security *(9:51 Minutes)*

In this module, learners are introduced to the concept of data security, its significance and the risks posed by insecure data handling. Other topics include: data classification, employee training, software security (antivirus and updates) and secure data storage, backup and recovery.

Everyone is responsible for data security.

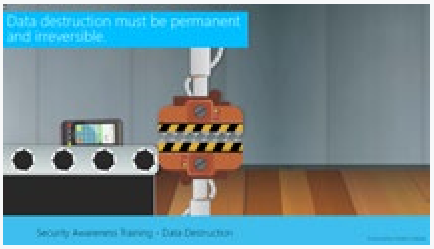
Data Retention *(4:32 Minutes)*

Our Data Retention module defines data retention in the context of information security and explains the value of a data retention plan in specific scenarios. It will walk learners through common data retention plans, data types typically subject to data retention policies and secure data disposal considerations.

Data classification is the foundation of a retention plan.

Data Destruction *(2:17 Minutes)*

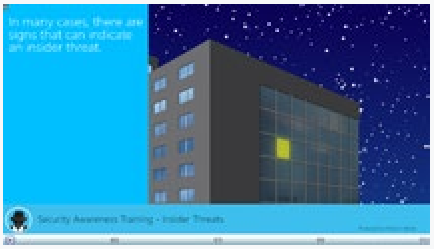
This module reinforces the importance of secure data-disposal methods and shares best practices for disposal of sensitive data. It defines what secure data destruction is and how data can be found in many forms and locations, and provides recommendations for secure data destruction methods.



Data destruction must be permanent and irreversible.

Insider Threats *(3:46 Minutes)*

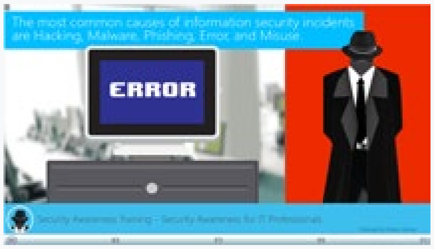
Insider threats include security threats posed by employees, contractors or vendors. This module explains why malicious insiders are dangerous, and provides examples of common behaviors that can be indicators of insider threats. Suggestions for incident reporting are also included to help combat insider threats.



In many cases, there are signs that can indicate an insider threat.

IT Staff *(10:37 Minutes)*

This module explains fundamental concepts of information security and the important role IT professionals play in protecting organizational data assets. It discusses some of the most common information security threats and motivations behind cyber attacks, and outlines fundamental goals of information security.



The most common causes of information security incidents are Hacking, Malware, Phishing, Error, and Misuse

ERROR
Security Awareness Training – Security Awareness for IT Professionals

Helpdesk *(5:00 Minutes)*

Our Helpdesk module explains how hackers can exploit the trust between a helpdesk and its users through social engineering attacks. Suggested methods for identifying and combating helpdesk-related social engineering attacks are included in the module.

Secure Application Development (OWASP Top 10) Modules

Role-based customization available for all staff levels, industries and departments.

Using Components with Known Vulnerabilities *(3:29 Minutes)*

Identifying vulnerabilities in commercial or open source software can be challenging, making security risk mitigation difficult. This module discusses use of components with known vulnerabilities (such as libraries and frameworks) that may undermine application defenses and enable various attacks.

Most web applications rely on third-party components.

Security Awareness Training -Using Components With Known Vulnerabilities

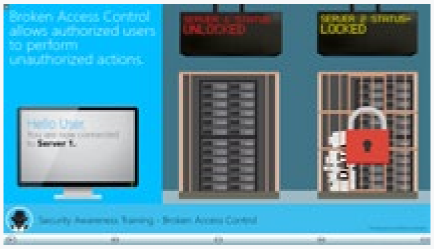
Underprotected APIs *(2:54 Minutes)*

Application programming interfaces (APIs) facilitate interaction between applications. Just like other applications, APIs can be subject to data theft, corruption and other attacks. This module defines underprotected APIs, explains why API security is important and discusses common attack methods and mitigation strategies.

APIs are widely used and often unprotected.

Broken Access Control *(3:00 Minutes)*

This module defines and explains broken access control, which allows attackers to access unauthorized functionality and/or data. We'll explain how broken access control can be leveraged to access others' accounts, view sensitive files, modify user data and change access rights.



Broken Access Control allows authorized users to perform unauthorized actions.

Cross-Site Request Forgery (CSRF) *(3:16 Minutes)*

Cross-Site request forgery (CSRF) occurs when hackers send unauthorized commands from a user's browser. In this module, we'll review common exploitation techniques and ways learners can protect applications from CSRF.

CSRF is used to trick users into submitting various malicious requests.

My Hacking Tools
<iframe>
XSS
Security Awareness Training - Cross-Site Request Forgery (CSRF)

Security Misconfiguration *(3:29 Minutes)*

In this module, we define security misconfiguration and offer tips on improving server security. We'll teach learners how to define secure settings for all application components, and explain the dangers of insecure defaults and outdated software.

Can you identify a sensitive data exposure vulnerability in the following examples? The same password is protected using different mechanisms.

Base64 encoded
SHA-256 hash with salt
AES 256 encrypted Base64 encoded
Argon2 hash with salt
Security Awareness Training - Security Misconfiguration

Injection *(4:25 Minutes)*

Injection is one of the most common, and harmful, security risks to web applications. This module details different types of injection and suggests effective mitigation strategies for the workplace.

Injection means any attack that involves inserting code into a web application.

Cross-Site Scripting (XXS) *(3:35 Minutes)*

Cross-site scripting (XXS) allows attackers to run scripts in a victim's browser to bypass access controls. In this module, we explain three types of XSS attacks and suggest XXS prevention measures.

XSS flaws occur when an application updates a web page with unescaped content from an untrusted user

Insufficient Attack Protection *(2:44 Minutes)*

Deploying sufficient attack protection is essential to keeping sensitive information safe from hacking attempts. In this module, we'll discuss web-application requirements regarding detection, prevention and response to both manual and automated attacks.

Automated and manual attacks should be detected and blocked

!
Invalid username or password
USerN@mE
•••••••••••••••
Security Awareness Training -Insufficient Attack Protection

Broken Authentication & Session Management *(4:39 Minutes)*

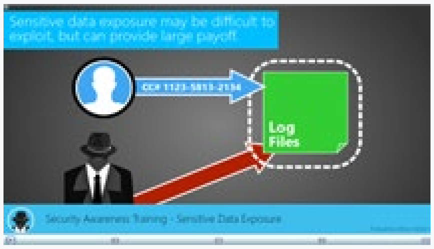
Managing usernames and passwords is an increasingly difficult, but necessary, task. This module describes what incorrect implementation of authentication and session management functions are, and explains how it can allow attackers to assume other users' identities. Included in the module are examples of attacks and general risk mitigation strategies.

Session management vulnerabilities can be attacked in many different ways

Security Awareness Training - Broken Authentication and Session Management

Sensitive Data Exposure *(3:47 Minutes)*

Our Sensitive Data Exposure module reinforces the need for security policies by outlining common risks of mishandled personal information. We'll reinforce the need for policy adoption by demonstrating how sensitive data, such as financial, healthcare and personal information, can be used to steal or modify information to conduct credit card fraud, identity theft or other crimes.



Sensitive data exposure may be difficult to exploit, but can provide large payoff

Security Awareness Training - Sensitive Data Exposure

Microlearning Videos

Our microlearning video series helps you reach learners with limited time or shorter attention spans.

Dumpster Diving *(1:03 Minutes)*

Dumpster diving is a technique used by hackers and thieves to steal sensitive data from organizations.This short, one-minute video outlines the risks improperly disposed printed material, technology and removable media can pose to an organization.

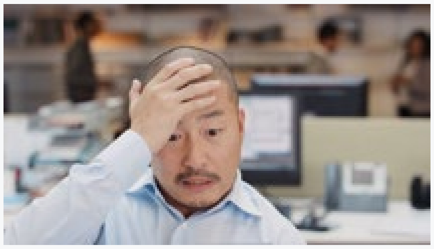
Printed material, technology and removable media must be shredded or destroyed before disposal
Security Awareness Training - Dumpster Diving

How Much Is Too Much? *(1:00 Minutes)*

In less than one minute, this video reinforces the importance of keeping passwords private. It uses actors, professionally produced scenes and compelling narrative to reinforce the consequences of poor password security.

One Wrong Move *(1:00 Minutes)*

This one-minute video uses actors, professionally produced scenes and compelling narrative to reinforce the consequences of a phishing attack.



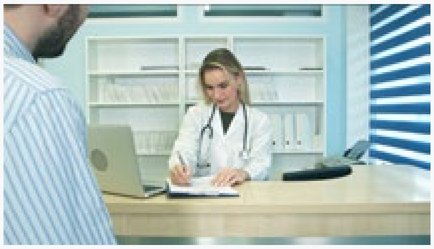
Is It Safe? *(1:00 Minutes)*

This short video reinforces the importance of using trusted publishers when installing mobile applications. It uses actors, professionally produced scenes and compelling narrative to reinforce the consequences of insecure mobile applications.

Who Can You Trust?

(1:00 Minutes)

In 60 seconds, this video highlights the risks of disclosing patient information without first verifying requester identity. It uses actors, professionally produced scenes and compelling narrative to reinforce the importance of keeping PHI safe.`



How Secure Is Public Wi-Fi?

(1:00 Minutes)

In just one minute, this video explains the risks of connecting to public Wi-Fi networks, including how sensitive information can be intercepted by attackers. It uses actors, professionally produced scenes and compelling narrative to reinforce the importance of secure network connections.

Where Is Your Device?

(1:00 Minutes)

This 60-second video details the importance of physical security and frequent data backups. It uses actors, professionally produced scenes and compelling narrative to reinforce the need to keep personal devices secure.

Additional Modules

Role-based customization available for all staff levels, industries and departments.

Intelligent Personal Assistant *(8:14 Minutes)*

As "intelligent" devices become increasingly integrated in personal and business settings, it is important to fully understand their impact to organizational security. This module defines Intelligent Personal Assistants and how they work, and explains some of the risks associated with using intelligent personal assistants in the workplace.

Click one of the options to continue
Security Awareness Training - Intelligent Personal Assistant

International Travel Security *(7:38 Minutes)*

This security awareness module introduces common information security risks found when traveling abroad. Travel preparation recommendations and best practices for data security in foreign countries are included in the module.

Take only what is necessary. Keep sensitive information in your carry on luggage.
Security Awareness Training - International Travel Security

Protecting Federal Tax Information *(8:06 Minutes)*

This module covers what federal tax information (FTI) is and why we need to protect FTI from unauthorized disclosure or access. It also outlines criminal and civil penalties for unauthorized disclosure of FTI (according to IRC sections 7213, 7213A and 7431) and what to do when a possible improper disclosure is discovered. Finally, we review best practices for avoiding unauthorized disclosure of FTI.

§7213
A fine of up to $5,000 and/or up to five years in jail for unauthorized disclosure
Security Awareness Training - Protecting Federal Tax Information

FERPA for K-12 *(7:14 Minutes)*

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. In this module, we identify who is impacted by FERPA, discuss the types of information that are protected by FERPA and detail what must be documented when a FERPA request is made. Specific regulations for K-12 institutions are highlighted.

FERPA for Post-Secondary Educators *(7:14 Minutes)*

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. In this module, we identify who is impacted by FERPA, discuss the types of information that are protected by FERPA and detail what must be documented when a FERPA request is made. Specific regulations for post-secondary institutions are highlighted.

The Family Educational Rights and Privacy Act, or FERPA, s designed to protect student information.

Security Awareness Training - FERPA for Post Secondary Education

Anti-Money Laundering Regulations (U.S.) *(10:02 Minutes)*

This interactive module explains money laundering — the criminal practice of hiding the true origin of illegally obtained cash. It introduces important U.S. laws and regulations intended to combat money laundering activities. Laws and regulations covered include the Bank Secrecy Act, the Money Laundering Control Act of 1986, The USA PATRIOT Act and FINRA Rule 3310 (Anti-Money Laundering Compliance Program).

Money laundering is the process of making illegally gained proceeds appear "clean".

Intellectual Property *(00:00 Minutes)*

This module covers the appropriate use of intellectual property. It introduces important intellectual property protection mechanisms (patents, trademarks, and copyrights) and how they apply to various types of products, including software and digital media.

Coming Soon

Vishing *(6:44 Minutes)*

This interactive training module covers voice phishing, or vishing, a simple but effective technique cyber criminals and scam artists use to collect confidential information. It explains what vishing is and what type of information it aims to gather. The module shares real-life vishing scenarios and provides recommendations for identifying and combating vishing attempts.

SMiShing *(4:58 Minutes)*

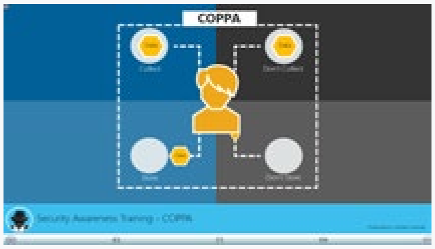
SMS Phishing, or SMiShing, is used by cyber criminals to collect valuable information and distribute malware. After completing this module, learners will know what SMiShing is, how to recognize a SMiShing attack and effective ways to stop SMiShing attempts.

SMiShing messages contain malicious links or attachments.

"You spent $1993.27 USD at The Home Shop. If you did not make this transaction please call us immediately at 1-408[illegible]23-4567. Thank You.

Children's Online Privacy Protection Act (COPPA) *(6:11 Minutes)*

This module covers the provisions of the Children's Online Privacy Protection Act (COPPA). It outlines when an organization is subject to COPPA requirements, and how to ensure compliance with COPPA provisions.



Additional Languages

Modules Now Available in Dutch:

1. Program Introduction
2. Program Conclusion
3. Privacy & EU GDPR
4. Malware
5. Phishing
6. Physical Security
7. Password Security
8. Working Remotely
9. Removable Media
10. Social Engineering
11. Mobile Security
12. Safe Web Browsing

Modules Now Available in Italian:

1. Program Introduction
2. Program Conclusion
3. Malware
4. Phishing
5. Physical Security
6. Password Security
7. Working Remotely
8. Removable Media
9. Social Engineering
10. Mobile Security
11. Safe Web Browsing

Modules Now Available in British English:

1. Program Introduction
2. Program Conclusion
3. Malware
4. Phishing
5. Physical Security
6. Password Security
7. Working Remotely
8. Removable Media
9. Social Engineering
10. Mobile Security
11. Safe Web Browsing

Modules Now Available in Russian:

1. Program Introduction
2. Program Conclusion
3. Malware
4. Phishing
5. Physical Security
6. Password Security
7. Working Remotely
8. Removable Media
9. Social Engineering
10. Mobile Security
11. Safe Web Browsing

Modules Now Available in Polish:

1. Program Introduction
2. Program Conclusion
3. Malware
4. Phishing
5. Physical Security
6. Password Security
7. Working Remotely
8. Removable Media
9. Social Engineering
10. Mobile Security
11. Safe Web Browsing

Modules Now Available in Romanian (Captions Only):

1. Program Introduction
2. Program Conclusion
3. Malware
4. Phishing
5. Physical Security
6. Password Security
7. Working Remotely
8. Removable Media
9. Social Engineering
10. Mobile Security
11. Safe Web Browsing

Modules Now Available in Bosnian:

1. Program Introduction
2. Program Conclusion
3. Malware
4. Phishing
5. Physical Security
6. Password Security
7. Working Remotely
8. Removable Media
9. Social Engineering
10. Mobile Security
11. Safe Web Browsing