Foreign Branch Office (FBO)

The Foreign Branch Office (FBO) series of courses covers key compliance topics that are must haves for employees of Foreign Branch Offices within the United States.

Recommended for:

- Asset Management
- Board of Directors
- Commercial
- Compliance - External Audit
- Compliance - Internal Audit
- Operations and IT
- Retail

FBO - Anti-Boycott

30 Minutes

This course explains the Anti-boycott Provisions of the Export Administration Act (EAA) and the Export Administration Regulations (EAR). The course explains what constitutes illegal boycott-related activities and your responsibilities regarding these provisions. The course also contains a scenario activity where you will be asked to use what you have learned to respond appropriately in a situation that may involve illegal boycott-related conditions.

FBO - Anti-Money Laundering (AML)

60 Minutes

This course explains the money laundering process and educates you about ways to prevent money laundering at your financial institution. It also discusses key legislation and your financial institution's requirements for its Anti-Money Laundering (AML) strategy.

FBO - Bank Bribery Act

30 Minutes

This course covers prohibitions against bank bribery. It discusses what type of items/gifts a financial institution's employee is forbidden to accept and lists a variety of exceptions. The course also contains a scenario with Anne Marie, a bank employee, and Mario, her customer. As you move through the scenario, you will be asked to determine if Mario is trying to bribe Anne Marie, and how Anne Marie's responsibilities and compliance requirements will determine how she is required to respond.

FBO - Bank Secrecy Act for Foreign Branch Offices

60 Minutes

The Bank Secrecy Act (BSA) helps the United States government combat money laundering and other illegal financial activity. All banks operating in the United States or U.S. Territories must adhere to these BSA rules and regulations. This course provides an overview of the BSA and discusses its identification, recordkeeping, and reporting requirements.

FBO - Customer Due Diligence and Enhanced Due Diligence (CDD/EDD)

30 Minutes

Customer due diligence (CDD) is a critical part of your branch's/agency's Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) policies. This course discusses the purpose of CDD guidelines and the basic way CDD can help you to know your customer, assess risk, and decide when enhanced due diligence (EDD) may be necessary. Employees must know how and when to apply appropriate CDD and EDD procedures. This course explains the basics of CDD and EDD and provides opportunities to practice what you have learned in two scenario activities.

FBO - Customer Identification Program (CIP)

90 Minutes

This course reviews the basic requirements of a Customer Identification Program (CIP) as prescribed by the PATRIOT Act. It explains the relationship between the CIP and the institution's Anti-Money Laundering (AML) program. In addition, it provides guidance on how to verify the identity of customers and how to respond to identify verification problems.

FBO - Embassy and Foreign Consulate Accounts

30 Minutes

This course explains why an embassy and foreign consulate may need an account in the United States. The course discusses the risks associated with an embassy or foreign consulate account and what a U.S.-based branch of a foreign bank can do to mitigate those risks.

FBO - Expedited Funds Availability Act: Regulation CC

60 Minutes

This course provides an overview of the Expedited Funds Availability Act (EFAA) implemented by Regulation CC. The course begins by introducing Regulation CC basics, and then covers the availability of funds. It also discusses Regulation CC exceptions.

FBO - Foreign Correspondent Bank Accounts

20 Minutes

This course explains why foreign correspondent accounts pose money laundering risks to your branch/agency. The course also discusses the BSA and USA PATRIOT Act requirements that you must follow for foreign correspondent banking transactions. At the end of the course, you will be asked to apply what you have learned in a case study scenario.

FBO - Office of Foreign Assets Control (OFAC)

60 Minutes

All U.S. individuals and businesses are required to comply with regulations sanctioned by the Office of Foreign Assets Control (OFAC). Among other things, these regulations block or restrict financial institutions from transactions with foreign persons, countries, or entities that are known or suspected to have ties to terrorist activity or drug trafficking. This course provides a working knowledge of the OFAC regulations, including what the OFAC regulations entail, what to do if someone is found to be prohibited from engaging in transactions with the U.S., and what it takes to be compliant under these regulations.

FBO - Trade Finance Fraud

30 Minutes

Trade finance fraud and money laundering, also referred to as trade-based money laundering (TBML), can be performed during the shipment, documentation, or purchasing of goods and services. This is a growing threat primarily in the international economy. All financial institution employees must be aware of the red flags that indicate fraud and TBML and procedures they can use to help fight this type of crime.

FBO - Wire Transfers

45 Minutes

A branch/agency may have to process the sending and receiving of wire transfers. Since wire transfers can be associated with money laundering, you must be able to identify red flags that may indicate criminal activity in an account. This course discusses risk factors associated with wire transfer activity and ways you can help prevent your branch/agency from falling prey to any illegal wire transfer activity.

OnCourse Unplugged

CFT/OnCourse Unplugged video compliance courses are revolutionizing the way employees learn about serious topics, including courses that will change the face of compliance training and learning for years to come. The series includes a library of core video compliance courses that are published and reviewed by our compliance experts to ensure clients have everything needed to stay compliant in a fun and engaging way.

Recommended for:

- Commercial
- Mortgage Professionals
- Operations and IT
- Retail
- Wholesale Banking

Unplugged: Anti-Money Laundering

15 Minutes

This course explains the money laundering process and educates you about ways to prevent money laundering at your financial institution.

Unplugged: BSA/AML Overview

10 Minutes

The Bank Secrecy Act (BSA) helps the United States government combat money laundering and other illegal financial activity. This course provides an overview of the BSA and discusses identification, recordkeeping, and reporting requirements of the BSA.

Unplugged: BSA/AML Program

10 Minutes

This course explains the importance of an effective BSA/AML program for your institution and provides detail surrounding the key pillars critical to an effective and compliant program.

Unplugged: Currency Transaction Reports

15 Minutes

This course focuses on the currency transaction reporting requirements of the Bank Secrecy Act (BSA).The primary purpose of the BSA is to prevent and detect money laundering activity through financial institutions and certain other businesses within the United States. This course teaches you about the requirements for determining whether or not a Currency Transaction Report (CTR) is applicable to a transaction. Also, you will learn about the necessary customer information required by the CTR form, and how to correctly fill one out for specific situations.

Unplugged: Defending Against Phishers

15 Minutes

To help your organization combat internet fraud, this course teaches about phishing threats with engaging videos to engage and train employees about these types of attacks and ways to handle them.

Unplugged: Equal Credit Opportunity Act

20 Minutes

This course presents the key points of the Equal Credit Opportunity Act (ECOA) and Regulation B requirements for all loan application, processing, evaluation, and notification processes. These regulations also have recordkeeping and reporting requirements.

Unplugged: Fair Housing Act

15 Minutes

This course explains how the Fair Housing Act (FHA) fights discrimination in the residential real estate lending process. The course discusses the lending prohibitions and the advertising requirements under the FHA.

Unplugged: Fair Lending Overview

15 Minutes

This course is intended to provide you with an understanding of the basic concepts regarding fair lending by explaining the fair lending laws and the penalties of breaking these laws.

Unplugged: Home Mortgage Disclosure Act

15 Minutes

This course is intended to provide you with an understanding of the basic concepts of the Home Mortgage Disclosure Act (HMDA). The course describes the primary requirements of HMDA and discusses the penalties for violations.

Unplugged: Identity Theft Program

15 Minutes

This course provides a fresh overview to the crime and prevention of identity theft. The concept of identity theft is presented, along with an understanding of the perpetrators and victims. The Fair Credit Reporting Act and Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act) establish the requirements for an Identity Theft Prevention Program. The key elements of this program are presented in this course.

Unplugged: Identity Theft Red Flags

15 Minutes

This course provides a fresh overview to the crime and prevention of identity theft. The concept of identity theft is presented, along with an understanding of the perpetrators and victims. The Fair Credit Reporting Act and Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act) establish the requirements for an Identity Theft Prevention Program. This course covers prevention techniques and identification of Red Flags of Identity Theft.

Unplugged: Know Your Customer

20 Minutes

This course reviews the basic requirements of a Know Your Customer (KYC). This includes the Customer Identification Program (CIP), Customer Due Diligence (CDD) procedures and Enhanced Due Diligence (EDD) procedures as prescribed by the USA PATRIOT Act. It explains the relationship between KYC and the institution's Anti-money Laundering (AML) program. In addition, it provides guidance on how to verify the identity of customers, and perform necessary due diligence.

Unplugged: OFAC

15 Minutes

All U.S. individuals and businesses are required to comply with regulations sanctioned by the Office of Foreign Assets Control (OFAC). Among other things, these regulations block or restrict financial institutions from transactions with foreign persons, countries, or entities that are known to have, or suspected of having, ties to terrorist activity or drug trafficking.

This course provides a working knowledge of the OFAC regulations. This includes discussing what is entailed by the OFAC regulations, what to do if someone is found to be prohibited from engaging in transactions with the United States, and what it takes to be compliant under these regulations.

Unplugged: Privacy

15 Minutes

This course presents the key points of the concepts, terms and requirements of the Gramm-Leach-Bliley (GLB) Privacy Rules as they apply to your financial institution and your job function. When an institution chooses to share nonpublic personal customer information with a nonaffiliated third party, a customer can opt out or forbid the sharing of his or her information. This course is for institutions that either share or don't share any of its customers' nonpublic personal information with nonaffiliated third parties outside of the permissible exceptions contained in the Privacy Rules.

Unplugged: Social Engineering

15 Minutes

This course introduces Social Engineering as it relates to information security. There are several techniques of social engineering that may be employed against staff members of a financial institution in attempt to gain access to customer information, company proprietary information, or other protected information.

Unplugged: Suspicious Activity Reports

15 Minutes

The Bank Secrecy Act (BSA) and its related laws exist primarily to prevent money laundering and other illegal financial activity. To comply with the BSA, all financial institution employees must be able to detect and report suspicious activity. This course defines and identifies several types of suspicious activity and discusses your reporting responsibilities.

Cybersecurity Starter

These courses deliver a strong beginning for your first security awareness program. It offers a simple solution with easy deployment, and particularly geared towards not very complex organizations with a lower threat level.

Recommended for:

- Asset Management
- Board of Directors
- Commercial
- Compliance - External Audit
- Compliance - Internal Audit
- Human Resources
- Mortgage Professionals
- Operations and IT
- Retail
- Wholesale Banking

Defending Against Phishers

12 Minutes

Because today's computers and networks are heavily defended from a direct assault, hackers are now much more likely to target end-users when trying to break in. If hackers can trick you into divulging your username and password or inadvertently infecting your computer with malicious software, they can use your computer as a launching point to further penetrate your organization's network. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for recognizing and preventing both phishing and spear-phishing attacks.

Security Awareness Essentials

30 Minutes

This course covers a high level overview of the major standards and topics of the NIST. Employees will master the fundamentals of information security including key threats and how to counter them. By mastering the information presented in this course, employees will be able to defend workplace data from malicious threats and become certified in basic security awareness. This security awareness training course covers key security best practices end users should follow so they can prevent, detect, and respond to information security threats.

Key Topics: Introduction, password management, identity theft, malware, social engineering, phishing, physical security, travel safety, mobile data, ransomware expansion, spear phishing expansion, and privacy and acceptable use updated statistics.

Cybersecurity Advanced

Our Cybersecurity Advanced series delivers the ability to target with role based courses, comply with special standards requirements, and to shift culture with a more advanced reinforcement strategy. For organizations who are ready to transform the workforce into a security-minded culture.

Recommended for:

- Asset Management
- Board of Directors
- Commercial
- Compliance - External Audit
- Compliance - Internal Audit
- Human Resources
- Mortgage Professionals
- Operations and IT
- Retail
- Wholesale Banking

A Day in the Life Theme: Security Awareness

70 Minutes

This course covers every topic required by major standards and regulations and is designed to change user behavior by diving deeply into each topic. Employees will master the fundamentals of information security including key principles, concepts, vulnerabilities, threats and how to counter them. By mastering the information presented in this course, employees will be able to defend personal and workplace data from malicious threats.

In this highly interactive course, learners will explore key information security concepts, examine threats and how to counter them and review safe computing habits that can be applied at home and in the workplace. By following the best practice lessons covered in this course, participants will be better able to recognize cyber threats and know how to defend against them.

Key Topics: Introduction, password management, viruses and malware, mobile data, physical security, social engineering, phishers, encryption, acceptable use policies incident response, backups, security services, risk management, network eavesdropping, protecting your home computer and identity theft.

A Day in the Life Theme

(with Adaptive TestOut/Analytics)

Individual

Learners take a test before the course starts, then based on those results, the course adapts so they are only presented with the course topics they don't know.

Appropriate Use of Social Media

14 Minutes

Social media can be an excellent tool to connect and interact with customers, show thought leadership, and build a brand, but it also poses unique security, HR, and public relations challenges. This course covers social media best practices including secure use, accountability, harassment, how to spot scams, secure passwords, and advanced security features. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for social media.

Baseline Information Security Training for IT Professionals

60 Minutes

This course is designed to provide fundamental information security knowledge that every employee in the IT Department must have in any organization. This course is easily customized to fit your particular policies, procedures, best practices and guidelines.

Cloud Security

9 Minutes

Cloud-based services offer incredible convenience and can help people be more productive, especially while on the go. But they also create new security challenges, because the security of any information stored on the cloud is only as good as the security of the service provider who holds it. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for cloud security.

Data and Records Retention

35 Minutes

Data in electronic and hard copy format within organizations is growing at a rate of about 125% per year and yet only 20% of that data is actually used to conduct business. Managing all of that data can become an administrative nightmare for you and the organization as a whole. This is especially true when litigation is pending and we must sift through all of our records to find certain pieces of data. This course will help you understand how to comply with the many laws, regulations, policies, and best practices that govern how long certain kinds of data should be kept and how and when to dispose of that data properly.

Defeating Social Engineers (Advanced)

17 Minutes

With increasingly sophisticated technical defenses for networks and computer systems, hackers often decide that it is much easier to simply go around these perimeter defenses by attacking the end user. After all, end users have what they want - a computer that's behind the network firewall, a network username and password, and possibly access to trade secrets, confidential information, and bank accounts. This course will teach end users how to identify and avoid giving away sensitive information to these hackers.

Defeating Social Engineers (Standard)

10 Minutes

With increasingly sophisticated technical defenses for networks and computer systems, hackers often decide that it is much easier to simply go around these perimeter defenses by attacking the end user. After all, end users have what they want - a computer that's behind the network firewall, a network username and password, and possibly access to trade secrets, confidential information, and bank accounts. This course will teach end users how to identify and avoid giving away sensitive information to these hackers.

Defending Against Phishers

12 Minutes

Because today's computers and networks are heavily defended from a direct assault, hackers are now much more likely target end-users when trying to break in. If hackers can trick you into divulging your username and password or inadvertently infecting your computer with malicious software, they can use your computer as a launching point to further penetrate your organization's network. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for recognizing and preventing both phishing and spear-phishing attacks.

Email Security and Instant Messaging Security

11 Minutes

Email and instant messaging (IM) are essential communication tools that most people use just about every day. They're incredibly useful applications because they allow you to quickly and efficiently exchange messages and files with just about anyone else in the world. However, it's a two-way street, meaning that since you can connect with anyone online, anyone else, including hackers and cybercriminals, can connect with you. This course teaches employees email and IM best practices.

GDPR: GDPR for Data Handlers

8 Minutes

The European Union's General Data Protection Regulation (GDPR) took effect on May 25, 2018, ushering in sweeping changes to requirements for any organization that collects, maintains, or processes the personal data of individuals residing in the EU. Compliance with the GDPR will affect all our organization's data handling activities, either directly or indirectly, and all staff whose responsibilities include use of PII will be expected to operate in accordance with the regulation's safeguards. This course will provide employees a general awareness of the GDPR's requirements and how they affect our day-to-day data processing activities, as well as helping them to recognize potential problems should they arise.

GDPR: How to Comply With the GDPR in the US

10 Minutes

The General Data Protection Regulation, or GDPR, contains principles for protecting the privacy of EU citizens' personal data. When it took effect in 2018, every organization, worldwide, that gathers, stores, or processes this data in any way, must comply with the strong data protections required under the GDPR. Upon completion of this module, learners will be able to recognize situations where the GDPR comes into play and what to do when they encounter data that falls under GDPR regulations in the US.

GDPR: Introduction and Overview

20 Minutes

This comprehensive course is delivered in a series of short, concise modules targeted to specific areas of the law and targeted to defined roles contained within the GDPR. Participants will learn the fundamentals of the new regulations and the key concepts behind them. By the end of this course series, learners will be able to recognize situations where the GDPR comes into play and what to do when they do encounter data that falls under GDPR regulations.

*Note: This course covers information for those who reside in an EU member country.

GDPR: Key Principles of the GDPR

15 Minutes

This comprehensive course is delivered in a series of short, concise modules targeted to specific areas of the law and targeted to defined roles contained within the GDPR. Participants will learn the fundamentals of the new regulations and the key concepts behind them. By the end of this course series, learners will be able to recognize situations where the GDPR comes into play and what to do when they do encounter data that falls under GDPR regulations.

*Note: This course covers information for those who reside in an EU member country.

GDPR: Navigating the GDPR with our US Partners

8 Minutes

The European Union's General Data Protection Regulation (GDPR) took effect on May 25, 2018, ushering in sweeping changes to requirements for any EU organization that collects, maintains, or processes the personal data of EU citizens, and exchanges of that data with organizations outside the EU will be significantly impacted. Since data transfers with the US represent a major share of these cross-border activities, this course will focus on a comparison of the differences between EU and US privacy laws, as well as exploring avenues by which EU-US information exchanges can be conducted.

GDPR: Transfers of Data Outside of the EU

8 Minutes

This course is one of a multi-part series that covers the fundamentals of the EU's General Data Protection Regulation, or GDPR, as well as its origins and key concepts. The GDPR contains principles for protecting the privacy of EU citizens' personal data. When it took effect in 2018, every organization, worldwide, that gathers, stores, or processes this data in any way, must comply with the strong data protections required under the GDPR. In this module, you learn how the GDPR affects our organization when transferring or receiving EU citizens' private information outside the borders of the UK and EU.

Human Firewall Theme

(with Adaptive TestOut/Analytics)

Individual

Learners take a test before the course starts, then based on those results, the course adapts so they are only presented with the course topics they don't know.

Human Firewall Theme: Security Awareness and Literacy

90 Minutes

This course covers every topic required by major standards and regulations, and is designed to change user behavior by diving deeply into each topic. Employees will learn the fundamentals of information security including key principles, concepts, vulnerabilities, threats and how to counter them. By mastering the information presented in this course they will be able to defend your personal and workplace data from malicious threats and become certified in information security awareness and literacy.

Key Topics: Introduction, password management, viruses and malware, mobile data, physical security, social engineering, phishers, encryption, acceptable use policies incident response, privacy and legal issues, security services, backups, risk management, network eavesdropping, protecting your home computer and identity theft.

Incident Reporting

7 Minutes

Reporting incidents of suspicious activity and the loss of assets or sensitive information is extremely important. In this module, employees will learn about common physical and information security incidents that should be reported and how to report them.

Information Security for Executives

14 Minutes

With the goal of breaching your network, cybercriminals have stepped up their efforts to target C-level executives, upper management and those with privileged access to an organization's systems with a variety of focused attacks. They are out to steal money, personal /credit info of clients and customers as well as intellectual property and other assets from organizations across the globe. And if yours is targeted, there may be more at stake than just loosing data. It may mean the CEO and other executives' jobs. This course focuses on what executives can do to help keep their organization safe and their business-reputation intact in the face of today's cybercriminals. Participants will explore key concepts of executive-level information security concerns and what you can do to bolster your organization's overall security posture.

Key Topics: Whaling, Business Email Compromise (BEC), Travel Security (Dark Hotel, Evil Twin, etc.), Protecting an Organization, Security Awareness Programs, Support Staff and Threat Landscape.

"Internet of Things" (IoT) and Home Security

10 Minutes

Almost anything can be made into a "smart" device, such as security cameras and sensors, TVs, garage door openers, door locks, wearable devices, pacemakers, and even cars. These devices are what we refer to as the "Internet of Things" (IoT), which holds the promise of adding a whole new level of convenience and connectedness to everyday life. Having that many new, connected computing devices, most of which record activity, presents new challenges for security and privacy. This course teaches employees the best practices for IoT devices both at home and at work.

OWASP Top 10 Web Application Vulnerabilities

15 Minutes

The Open Web Application Security Project (OWASP is a global community focused on improving the security of web application software. The OWASP Top Ten list is highly respected and has been adopted by, among other organizations, the Payment Card Industry (PCI) Security Standards Council. This short lesson reviews the top ten list to ensure all web application developers in your organization are exposed to it.

Password Management

15 Minutes

Passwords are the keys to our digital lives and protect us from hackers and cybercriminals, but how exactly could a hacker crack your password and what can you do to protect it? This HTML5-based, iPad-compatible password management course uses high-quality video and real-world simulations to show the tactics hackers use to compromise accounts and the password security best practices that can help prevent that from happening.

PCI Essentials for Cardholder Data Handlers and Supervisors

25 Minutes

This course teaches employees and supervisors what PCI DSS is, how it affects your organization and the best practices they should follow to protect cardholder data and detect and prevent fraud. This course is meant for employees and supervisors in companies that require PCI DSS – 3.2 compliance.

PCI Requirements Overview for I.T. Professionals

40 Minutes

This course teaches I.T. professionals what PCI DSS is, how it affects your organization, how to comply with the 12 requirements and the best practices that front line staff should follow to protect cardholder data and detect and prevent fraud. This course is meant for IT Professionals in companies that require PCI DSS - 3.2 compliance.

Physical Security

10 Minutes

Your personal safety at work is of paramount importance. This course is designed to teach employees how to protect an organization from criminals, espionage, workplace violence, natural disasters, and other threats. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach physical security best practices.

Privacy and Data Protection

30 Minutes

This course will help employees understand what information is private, why it is private, and what they can do to protect it throughout the data lifecycle, which is the life of a piece of information, whether in paper or digital format, from creation to destruction within an organization.

Privileged User Security

20 Minutes

Hackers and cybercriminals specifically target privileged users. After all, they have access to an organization's most prized data. This course will teach privileged users the security best practices they're expected to follow in order to defend against hackers.

Protecting Mobile Data and Devices

8 Minutes

Because today's smartphones and tablets can not only act as a phone, but also as an email client, mobile Internet device, camera, GPS navigation system, entertainment console, and platform for any number of applications (apps), they can be exposed to many of the same risks as a desktop computer. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach best practices for mobile security.

Security Awareness Essentials

30 Minutes

This course covers a high level overview of the major standards and topics of the NIST. Employees will master the fundamentals of information security including key threats and how to counter them. By mastering the information presented in this course, employees will be able to defend workplace data from malicious threats and become certified in basic security awareness. This security awareness training course covers key security best practices end users should follow so they can prevent, detect, and respond to information security threats.

Key Topics: Introduction, password management, identity theft, malware, social engineering, phishing, physical security, travel safety, mobile data, privacy and acceptable use updated statistics, ransomware expansion, spear phishing expansion.

Security Awareness for Managers

30 Minutes

This course is designed to educate managers to lead by example and encourage their teams to conduct everyday business in a responsible and secure way that reduces organizational risk, increases productivity and complies with policies, laws and regulations. Because they are the voice of your organization to their direct reports, your managers are in a unique position to influence the success or failure of your security awareness program, and their behavior and buy-in is a critical component of ensuring your cultural transformation to a security conscious organization.

Key Topics: Introduction, leading by example, security management practices and legal issues.

Security Awareness for the Home

7 Minutes

Threats to our home network can quickly turn into threats to our workplace infrastructure and visa-versa. To combat against threats on all fronts, we must learn to practice safe computing habits both in the home and in the workplace. In this course, participants will be introduced to some key principles of safe system administration that they can use in the home that mirror techniques used in the workplace. By mastering the techniques found in this course, participants will learn to develop a regime of security-conscience behavior that will help keep important data safe from hackers, data thugs and cybercriminals.

Security Awareness Fundamentals Theme

(with Adaptive TestOut/Analytics)

Individual

Learners take a test before the course starts, then based on those results, the course adapts so they are only presented with the course topics they don't know.

Strongest Link Theme
(with Adaptive TestOut/Analytics)

Individual

Learners take a test before the course starts, then based on those results, the course adapts so they are only presented with the course topics they don't know.

Strongest Link Theme: Security Awareness and Literacy

50 Minutes

This course covers every topic required by major standards and regulations, and is designed to change user behavior by diving deeply into each topic. Employees will master the fundamentals of information security including key principles, concepts, vulnerabilities, threats and how to counter them. By mastering the information presented in this course, employees will be able to defend personal and workplace data from malicious threats.

Key Topics: Introduction, password management, viruses and malware, mobile data, physical security, social engineering, phishers, backups, acceptable use policies incident response, privacy and legal issues, security services, risk management, network eavesdropping, encryption, protecting your home computer and identity theft.

Working Remotely

12 Minutes

Mobile computing devices like laptops, smartphones, and tablets can be found everywhere - at home, in the office, and everywhere in between. These devices, combined with high speed wireless connections, make working remotely easier than ever. However, working outside of a company's secured facilities expose an organization's physical and information assets to additional threats. This course gives the best practices for working remotely.