inspired eLearning
education for your enterprise

STOP THE ATTACKS
START PROTECTING YOUR BUSINESS

FINDING A SOLUTION

Companies spend millions of dollars and countless hours every year on technology to protect their IT systems, but cyber-attacks continue to happen. Organizations are looking for an answer to protect themselves from these ongoing attacks so that their customer data or proprietary information does not fall into the hands of malicious hackers. The answer is education. People are the weakest link in the firewall around these IT systems. Attacks are squarely centered on taking advantage of this weakest link and exploiting that lack of knowledge around security.

Training employees, as simple as it sounds, is where the prevention concept can break down. Training cannot be approached as a "one and done." It must be a continuum of knowledge. Threats will always manifest in different ways. Employee education must reflect the evolving threat.

Inspired eLearning delivers a holistic cyber-security training solution equipping employees with the necessary armor to readily handle front-line attacks that continually exploit the human weakness in IT systems.

WHAT DOES **READY** LOOK LIKE?

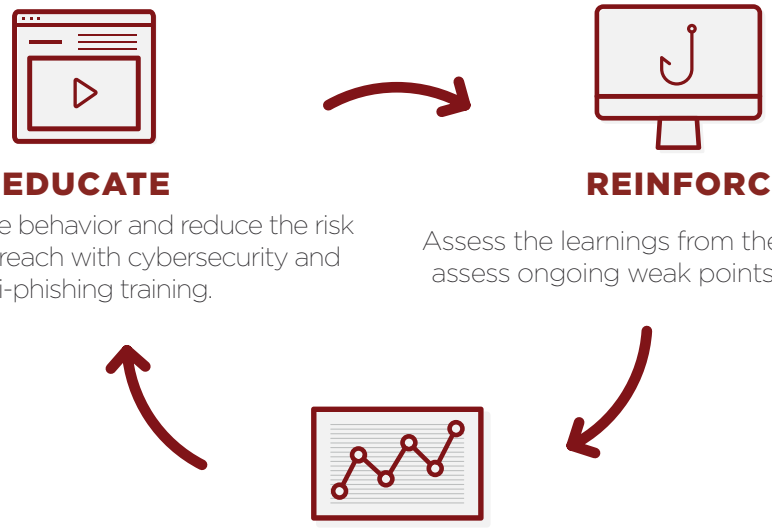
Ready looks like a workforce that has internalized the importance of security. It looks like an organization whose employees habitually use safe practices by recognizing and effectively reacting to dangerous situations.

Your employees now form a human firewall, allowing you to focus on your core business. With deeply rooted awareness training, they are free to focus on their work. That's what **ready** looks like.

Inspired eLearning enables your company to educate, empower and transform your organization. Our award-winning security training helps create that human firewall against cyber-attacks, making your organization **ready.**

THE INSPIRED SECURITY SOLUTION

Inspired eLearning provides a complete solution to the training needs of your organization. The solution is based on three simple fundamentals:



EDUCATE

Change employee behavior and reduce the risk of a security breach with cybersecurity and anti-phishing training.

REINFORCE

Assess the learnings from the training and assess ongoing weak points in the system.

ANALYZE

Analyze the results at all steps along the process.

A vital component to this entire solution is the reinforcement phase and where PhishProof fits in. PhishProof simulates phishing attacks to identify weak spots in your employee base and gives users training when it is most effective — the moment they click. This just-in-time training is more time efficient and cost effective, offering a greater return on training investment. **Inspired eLearning** assessments and training have reduced phishing susceptibility by more than 92%.

PhishProof is available as a completely managed service where our team of experts design and deploy assessments and training to your specifications, or as a Software-as-a-Service model where you can use the powerful, user-friendly software to build and deploy your own assessment within minutes.

INSPIRED eLEARNING

Inspired eLearning offers solution packages and multi-year training options that bring your company into the future of security awareness training now.

- **Solution packages**
- **Targeted and adaptive training**
- **ROI analytics**
- **Multiple compliance solutions**
- **Flexible training platforms**
- **Localized in 40+ languages**

Contact **Inspired eLearning** today to learn more about the **Inspired Security Solution** and making your organization **ready** to repel cyber-attacks. Contact us at **sales@inspiredelearning.com** or call us at **800-631-2078.**

STOP THE PHISHING

START PROTECTING YOUR BUSINESS

THE MOST COMPREHENSIVE ANTI-PHISHING PROGRAM AVAILABLE

PREVENT PHISHING ATTACKS TO YOUR ORGANIZATION

Phishing has become the most common method of cyberattacks. Phishers typically create fake emails that appear to come from a sender the user trusts, such as a bank, credit card company, or a popular website. These emails try to trick the user into giving away sensitive information, such as usernames, passwords, and credit card details.

What makes phishing so effective for hackers and cybercriminals, and therefore dangerous to any organization, is that phishing emails often bypass firewalls, spam filters, and antivirus software, and land in employees' inboxes. And if even one employee takes the bait, the organization's security will be compromised.

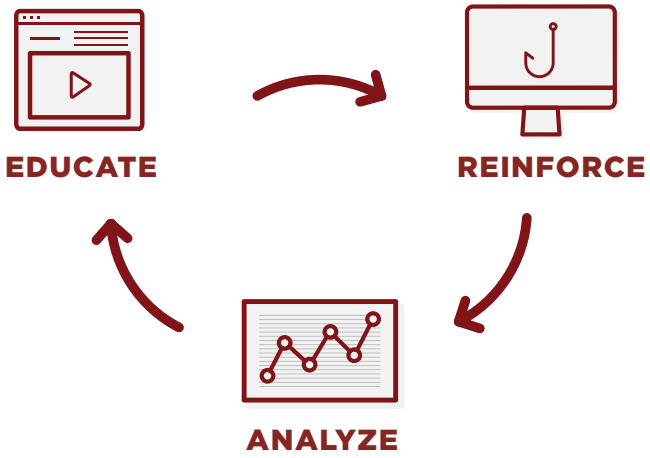
Inspired eLearning's security solution is designed to train your employees to avoid those disasters. With the PhishProof Anti-Phishing software as the cornerstone of the solution, you can quickly assess the weak points in your organization, and provide immediate training on how to avoid phishing attacks.

HOW DOES PHISHPROOF WORK?

Are your end-users susceptible to phishing or spear-phishing attacks? Make your end-user population a powerful defense and a human firewall by training them to recognize and respond to phishing threats immediately with Inspired eLearning's security training and PhishProof Anti-Phishing simulator.

Phishproof is designed to identify weak spots and give your employees training when it is most effective — the moment they click. This just-in-time training is more time efficient and cost effective, offering a greater return on training investment. Our assessments and training have reduced phishing susceptibility by more than 92%.

PhishProof is available as a completely managed service where our team of experts design and deploy assessments and training to your specifications, or as a Software-as-a-Service model where you can use the powerful, user-friendly software to build and deploy your own assessment within minutes.



EDUCATE

Change employee behavior and reduce the risk of a security breach with cybersecurity and anti-phishing training.

REINFORCE

Send out mock phishing attacks to employees.

ANALYZE

Evaluate phishing results and identify opportunities to reinforce training.

A PROVEN LEADER

Inspired eLearning's Security Awareness Training has been named a leader in Gartner's Magic Quadrant for Security Awareness CBT for the third year in a row. More than 15,000 enterprises have relied on Inspired eLearning to deliver the right security training for their organizations.

When you combine PhishProof with Inspired eLearning's security courses, you bring to your organization a robust and comprehensive security training program that delivers:

- **Targeted and adaptive training**
- **Flexible training platforms**
- **ROI Analytics**
- **Multiple compliance solutions**
- **Customization**
- **Localized in 40+ languages**

Contact **Inspired eLearning** today to learn more about how you can use **PhishProof** to fortify your organization against cyber-attacks. Contact us at **sales@inspiredelearning.com** or call us at **800-631-2078.**

inspired eLearning
education for your enterprise

Security Awareness Solution Features by Package

	Starter	Fundamentals	Advanced
Foundational Curriculum for all users			
Fundamentals - *major standards covered in 30 mins*	✓	✓	✓
Optional Themes - *major standards covered in more depth*		2	3
Training assessments (course tests)	✓	✓	✓
TestOut/Adaptive mode option			✓
Targeted Role Based curriculum			
Manager			✓
Executive			✓
IT & Developer			✓
Privileged User			✓
Intro to OWASP Top 10			✓
Standards & Compliance			
major standards for all users	✓	✓	✓
PCI for Cardholders & Supervisors		✓	✓
PCI for IT Professionals			✓
Privacy & Data Retention			✓
Data & Records Retention			✓
Interactive micro-learning for on-demand, targeting, remediation, and reinforcement			
Phishing	✓	✓	✓
Social Engineering		✓	✓
Mobile Security		✓	✓
Social Media		✓	✓
Working Remotely			✓
Password Management			✓
Physical Security			✓
Email Security			✓
Cloud Security			✓
Internet of Things/IoT			✓
Incident Reporting			✓
Mini videos covering topics above		add-on	add-on
Phishing Simulation Solution			
Unlimited simulated phishing campaigns	add-on	✓	✓
Susceptible users remediation & analytics	add-on	✓	✓
Browser & OS Analysis	add-on	✓	✓
Trend over time analysis	add-on	✓	✓
Suspicious email alert (Outlook plug-in)		✓	✓
Training Reports & Security Competency Analytics			
Security Awareness Competency Threat Profile	✓	✓	✓
TestOut/Adaptive time savings ROI analysis			✓
Learner completion status, scores	✓	✓	✓
Additional Features			
Off-the-Shelf Multilingual	✓	✓	✓
Supplemental Reinforcement Materials (*Tips, Best Practices, Posters, etc)*	✓	✓	✓
Policy Delivery & Acceptance Delivery/Tracking	✓	✓	✓
Learner Site Branding	✓	✓	✓
Deployment Management & Services			
hosting via dedicated Security Awareness platform	✓	✓	✓
Administrators Technical Support	✓	✓	✓
Deployment Strategy Planning & Guidance	✓	✓	✓
Self-service administrative controls and admin training	✓	✓	✓
Content Provision & Site Administration services	✓	✓	✓
Reports & Analytics Access	✓	✓	✓
Learner enrollment and due date emails	✓	✓	✓
Supervisor due date and progress emails for staff	✓	✓	✓
Training deadline enforcement	✓	✓	✓
Single Sign On option	✓	✓	✓

inspired eLearning
education for your enterprise

Starter	Fundamentals	Advanced	Type	Title	ID	Description	Duration (minutes)	Threat Analytics Profile	Test/Assess	Policy Link (option)
-	-	-	**Multi-Topic Foundational All-User**			*Also see the 'Foundational Themes Detail' worksheet for more info on these courses.*				
Yes	Yes	Yes		**Security Awareness Essentials Theme**	S-141-SA-01.18	Choose S-141 if you would like to deploy one course that covers every topic required by major standards and regulations in 30 minutes or less. 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 (30 mins): 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.	30	yes	yes	yes
		Yes		**Security Awareness Fundamentals Theme (with Adaptive TestOut/Analytics)**	S-141-TO	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.	individual	no	yes	yes
	Yes	Yes		**Human Firewall Theme: Security Awareness and Literacy**	S-103	Choose S-103 if you would like to deploy one course that covers every topic required by major standards and regulations, and if you want a course 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 (Appr.85-95 mins): Introduction, password management, viruses and malware, mobile data, physical security, social engineering, phishers, acceptable use policies incident response, security services, risk management, network eavesdropping, encryption, malware, backups, protecting your home computer,	85-95	yes	yes	yes
		Yes		**Human Firewall Theme (Adaptive TestOut/Analytics)**	S-103-TO	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.	individual	no	yes	yes
	Yes	Yes		**Strongest Link Theme: Security Awareness and Literacy**	S-133-SL-01-EN	Choose S-133 if you would like to deploy one course that covers every topic required by major standards and regulations, and if you want a course 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 (50-60 minutes) Introduction, password management, viruses and malware, mobile data, physical security, social engineering, phishers, acceptable use policies incident response, security services, risk management, network eavesdropping, encryption, malware, backups, protecting your home computer, identity theft, privacy and legal issues.	50	yes	yes	yes
		Yes		**Strongest Link Theme: (with Adaptive TestOut/Analytics)**	S-133-TO	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.	individual	no	yes	yes
		Yes		**A Day In the Life Theme: Security Awareness**	S-173	Choose S-173 if you would like to deploy one course that covers every topic required by major standards and regulations and if you want a course 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 (Appr.65-75 mins) Introduction, password management, viruses and malware, mobile data, physical security, social engineering, phishers, acceptable use policies incident response, security services, risk management, network eavesdropping, encryption, malware, backups, protecting your home computer, and identity theft.	65-75	yes	yes	yes

Starter	Fundamentals	Advanced	Type	Title	ID	Description	Duration (minutes)	Threat Analytics Profile	Test/Assess	Policy Link (option)
		Yes		**A Day In the Life Theme:(with Adaptive TestOut/Analytics)**	S-173-TO	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.	individual	no	yes	yes
-	-	-	**Single Topic iModules**							
Yes	Yes	Yes		**Phishing**	S-161-AP	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.	12		yes	no
	Yes	Yes		**Defeating Social Engineers (Standard or Advanced)**	S-161-SEA	With increasingly sophisticated technical defenses for networks and computer systems, hackers often decide that it's 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. This HTML5-based, iPad-compatible course uses	10; 17		yes	no
	Yes	Yes		**Protecting Mobile Data and Devices**	S-161-MD	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	8		sim	no
	Yes	Yes		**Appropriate Use of Social Media**	S-161-SM	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.	14		yes	no
		Yes		**Working Remotely**	S-161-WR	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	12		sim	no
		Yes		**Password Management**	S-161-PM	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	15		sim	no
		Yes		**Physical Security**	S-161-PS	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.	10		yes	no
		Yes		**Email Security & Instant Messaging Security**	S-161-ES	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 the email and IM best practices to protect	11		sim	no
		Yes		**Cloud Security**	S-161-CS	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	9		sim	no

Starter	Fundamentals	Advanced	Type	Title	ID	Description	Duration (minutes)	Threat Analytics Profile	Test/Assess	Policy Link (option)
		Yes		**Internet of Things" & Home Security**	S-161-HS	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. (10 minutes)	10		sim	no
		Yes		**Incident Reporting**	S-161-IR	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.	7		yes	pledge
-	*add-on*	*add-on*	**Micro-Learning' Mini Modules**							
				In-Person Social Engineering	S-161-SE-04	Social engineering attacks can often occur in person. In-person social engineers will use information obtained both online and offline, along with lies and manipulation, to gain access to your systems and facilities. This HTML5-based, iPad-compatible module uses high-quality video and real-world simulations to teach you how to defend against in-person social engineering attacks.	4		sim	no
				Social Engineering – How It Works	S-161-SE-03	The more you learn about how social engineering works, the better you can defend yourself and your organization against social engineering attacks. This HTML5-based, iPad-compatible module uses high-quality video and real-world simulations to teach you how to avoid being tricked into giving away sensitive information to social engineers.	4		sim	no
				Online and Targeted Social Engineering	S-161-SE-05	Social engineers may use both technical and non-technical methods in a "targeted attack," aimed at select individuals. Because these attacks are so tailored, they can be very difficult to recognize and therefore, very effective. This HTML5-based, iPad-compatible module uses high-quality video and real-world simulations to teach you how to protect against online and targeted social engineering attacks.	4		sim	no
				Social Engineering - Countermeasures and Incident Response	S-161-SE-06	Understanding what to do in the event of a social engineering attack can be just as important as prevention. Utilizing effective countermeasures and incident response procedures will help you to avoid falling prey to social engineers. This HTML5-based, iPad-compatible module uses high-quality video to teach you effective social engineering countermeasures and incident response best practices.	4		yes	no
				Appropriate Use of Social Media	S-161-SM-02	Properly used, social media can be a great asset to any organization. However, there are many pitfalls associated with using social media, especially since these sites tend to blur the lines between what's personal and professional. This HTML5-based, iPad-compatible module uses high-quality video and real-world simulations to teach you how to appropriately use social media.	5		yes	no
				Secure Use of Social Media	S-161-SM-04	Improper use of social media can also expose you to a wide range of security and privacy issues, malicious software, and scams. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach you best practices for the secure use of social media.	4		yes	no
				Social Media Best Practices	S-161-SM-03	When you post a comment, file, image and video to social media platforms, you never really know who'll wind up seeing it. Whatever you choose to express can also be quickly copied and spread far and wide with or without your knowledge. This HTML5-based, iPad-compatible course uses high-quality video and real-world simulations to teach you simple yet effective social media best practices.	4		yes	no
				Outwitting Internet Phishers	S-161-AP-02	Phishers will typically send fake emails that appear to come from someone you trust, such as a bank, credit card company, or popular website. The email may ask you to "confirm your account details" and direct you to a website that looks just like the real website, but whose sole purpose is stealing your information. This HTML5-based, iPad-compatible module uses high-quality video and real-world simulations to teach you best practices for recognizing and preventing phishing attacks.	7		yes	no
				Outwitting Spear Phishers	S-161-AP-03	Whereas Internet phishers target a wide audience by sending their fake emails to any address they can find, Spear Phishers target a select group, or a few individuals, with a highly tailored message. This method is much harder to counter because the email messages can seem so authentic. This HTML5-based, iPad-compatible module uses high-quality video and real-world simulations to teach you best practices for recognizing and preventing spear-phishing attacks.	4		yes	no
				An Introduction to Insider Threats	S-161-IT-02	Across the globe, organizations spend countless hours working to keep sensitive data out of the hands of cybercriminals. This task has become even more difficult to manage due to an increasing number of data compromises that stem from insider threats. This threat from within, or "insider threat" can be successfully addressed using the strategies shared in this module. In this module we will discuss the three types of insider threats, some recognizable behaviors associated with each type and provide simple yet effective strategies to counteract each threat.	7		yes	no

Starter	Fundamentals	Advanced	Type	Title	ID	Description	Duration (minutes)	Threat Analytics Profile	Test/Assess	Policy Link (option)
				Protecting Kids From Cyberbullying	S-161-KD-03	Cyberbullies use electronic communications to torment others with an onslaught of teasing, humiliation, and threats to do harm. Research suggests that cyberbullying may be a preferred attack method due to the perceived anonymity of the Internet. Fortunately, by applying the recommendations presented in this module you can help prevent cyberbullying. In this module we will discuss the effects of cyberbullying, some recognizable behaviors associated with cyberbullying and provide simple yet effective prevention strategies.	4		yes	no
				Protecting Mobile Devices and Data	S-161-MD-02	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.	4		sim	no
				Additional Best Practices for Mobile Devices	S-161-MD-03	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 additional best practices for mobile security.	4		sim	no
				Ransomware: How to Defend Yourself	S-161-MA-03	Ransomware is a type of malicious software used by hackers to encrypt files and other functions from a user until the victim pays a "ransom." This form of cyberattack has become one of the most used and most costly threats to businesses and individuals alike. By mastering the information presented in this course you will be able to help defend your personal and workplace data from ransomware threats.	4		sim	no
				Protecting Against Malicious Insiders	S-161-IT-03	The threat is real. It's taking place somewhere, right now. A malicious insider has decided to mount a cyberattack against your organization from the inside out. This malicious insider will stop at nothing to get the data they need to commit theft, fraud or sabotage. By applying the strategies provided in this modules and being willing to take action you can help rid the workplace of these malicious insider threats. In this module you will learn what a malicious insider does, some recognizable threat indicators and simple yet effective ways to address the malicious insider threat.	8		sim	no
				Preventing Malware (Mobile Devices)	S-161-MA-05	Mobile devices, including smartphones and tablets, have become so common in the workplace that many organizations now consider them essential tools. Unfortunately, mobile devices come with many of the same malware threats as computers and laptops, and even some of their own, including malicious app downloads. This course acknowledges the commonplace usage of mobile devices at work and explains key vulnerabilities that users must be aware of. By mastering the information presented in this course you will be able to help defend your mobile devices from security threats.	3		sim	no
				The Malware Threat	S-161-MA-02	Malware is any type of software that is intended to damage or disable computer systems. It is often used to steal information, destroy or lock users from data, or disrupt operations. This course defines malware and the associated security threats, and describes common types of malware. By mastering the information presented in this course you will be able to help defend your personal and workplace data from these threats.	5		sim	no
-	-	-	**Role-Based Courses**							
		Yes		**Security Awareness for Managers**	S-110	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 (30 minutes) Introduction, leading by example, security management practices and legal issues.	30		yes	no

Starter	Fundamentals	Advanced	Type	Title	ID	Description	Duration (minutes)	Threat Analytics Profile	Test/Assess	Policy Link (option)
		Yes		**Information Security for Executives**	S-114	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 (14 minutes) Whaling, Business Email Compromise (BEC), Travel Security (Dark Hotel, Evil Twin, etc.), Protecting an Organization, Security Awareness Programs, Support Staff, and Threat Landscape.	14		no	no
		Yes		**Privileged User Security**	S-111	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.	20		yes	no
		Yes		**Baseline Information Security Training for IT Professionals**	S-123-IT-01-EN	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 & guidelines.	60		yes	no
		Yes		**Introduction to the OWASP Top 10**	S-126	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.	15		yes	no
	-	-	**Standards & Compliance**							
	Yes	Yes		**PCI Essentials for Cardholder Data Handlers and Supervisors**	PCI-101	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.	25		yes	yes
		Yes		**PCI Requirements Overview for I.T. Professionals**	PCI-120	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.	40		yes	yes
		Yes		**Privacy and Data Protection**	P-101	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.	30		yes	yes
		Yes		**Data & Records Retention**	DR-101	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.	35		yes	yes