COURSE MODULES

Fortinet Security Awareness and Training Service

Base Training Modules

Training modules are approximately eight-minute interactive modules that are designed to teach students via multimedia interactive presentations and exercises. Courses include quizzes and assessments.

	Standard Service	Premium Service
Information Security Awareness	✓	✓
Bad Actors	✓	✓
Social Engineering	✓	✓
Phishing Attacks	✓	✓
Email Security	✓	✓
Malware and Ransomware	✓	✓
Password Protection	✓	✓
Multi-factor Authentication		✓
Data Security		✓
Data Privacy		✓
Access Control		✓
Mobile Security		✓
Insider Threat		✓
Clean Desk Policy		✓
Working Remotely		✓
Web Conference Security		✓
Business Email Compromise		✓
Intellectual Property		✓
Secure Travel Tips		✓
Social Media		✓
Managers: Information Security Frameworks		✓
Managers: Information Security Awareness		✓
Managers: Deploying and Managing the Fortinet Security Awareness and Training Service		✓

Micro Training Modules

Micro modules are a summary of the base modules, typically less than two minutes each, which are used as a follow-up to the base modules to reinforce a specific topic.

	Standard Service	Premium Service
Social Engineering	✓	✓
Phishing Attacks	✓	✓
Email Security	✓	✓
Malware and Ransomware	✓	✓
Password Protection	✓	✓
Data Security		✓
Data Privacy		✓
Business Email Compromise		✓
Insider Threat		✓
Clean Desk Policy		✓

Nano Training Modules

Typically less than one minute, nano modules can be used to reinforce a topic or as aids/assets to promote security awareness throughout an organization.

	Standard Service	Premium Service
Shoulder Surfing	✓	✓
Tailgating	✓	✓
See Something, Hear Something, Say Something	✓	✓
Follow Company Policy	✓	✓
Avoid Unknown Wi-Fi Networks	✓	✓
Good Password Hygiene	✓	✓
Think Before You Click	✓	✓
Web Conference Tips		✓
Travel Tips		✓
Back Up Your Data		✓
Data Disposal		✓
Disable Automatic Wi-Fi		✓
Encrypt Sensitive Data		✓
Enable Screen Locks		✓
Update Your Software		✓
Protect Your Devices		✓
Non-discoverable Bluetooth		✓
Use Multi-factor Authentication		✓

Base Modules by Theme Grouping

PREMIUM SERVICE

STANDARD SERVICE

	InfoSec Awareness	Data Privacy	Internet Security	Password Protection	Physical Security
Information Security Awareness	✓				
Bad Actors	✓		✓		
Social Engineering	✓		✓		✓
Phishing Attacks	✓	✓	✓	✓	
Email Security	✓	✓	✓		
Malware and Ransomware	✓		✓		
Password Protection	✓	✓		✓	
Multi-factor Authentication	✓	✓		✓	
Data Security	✓	✓	✓	✓	✓
Date Privacy	✓	✓			
Access Control	✓	✓			✓
Mobile Security	✓		✓	✓	
Insider Threat	✓	✓	✓	✓	✓
Clean Desk Policy	✓	✓			✓
Working Remotely	✓	✓	✓		
Web Conference Security	✓		✓		
Social Media	✓	✓	✓	✓	
Business Email Compromise	✓	✓	✓	✓	
Intellectual Property	✓	✓			
Secure Travel Tips	✓		✓		✓
Managers: Information Security Framework	✓	✓	✓		
Managers: Information Security Awareness	✓	✓			
Managers: Implementing the Service	✓				

Micro-Modules by Theme Grouping

PREMIUM SERVICE

STANDARD SERVICE

	InfoSec Awareness	Data Privacy	Internet Security	Password Protection	Physical Security
Social Engineering	✓		✓		✓
Phishing Attacks	✓	✓	✓	✓	
Email Security	✓	✓	✓		
Malware and Ransomware	✓		✓		
Password Protection	✓	✓		✓	
Data Security	✓	✓	✓	✓	✓
Data Privacy	✓	✓			
Business Email Compromise	✓	✓		✓	
Insider Threat	✓	✓	✓	✓	✓
Clean Desk Policy	✓	✓	✓		✓

Course Descriptions

Module Name	Description
Access Control	At the end of this short lesson, your students will be able to do the following: ▪ Describe access control and zero trust strategies ▪ Describe authentication, authorization, and accounting ▪ List the main types of access control ▪ Describe the importance of access control ▪ List actions to take
Bad Actors	At the end of this short lesson, your students will be able to do the following: ▪ Identify the types of bad actors ▪ Understand bad actor motives ▪ List actions to prevent a cybersecurity attack ▪ Understand the people who are bad actors
Business Email Compromise	At the end of this short lesson, your students will be able to do the following: ▪ Describe common strategies used by bad actors to compromise your business email security ▪ Identify the different stages of a Business Email Compromise (BEC) attack ▪ List actions that you can take to protect yourself from a BEC attack
Clean Desk	At the end of this short lesson, your students will be able to do the following: ▪ Describe risks ▪ Define the clean desk principle ▪ List examples of adherence to the clean desk principle ▪ List actions to take to secure information at your workspace
Data Privacy	At the end of this short lesson, your students will be able to do the following: ▪ Describe data privacy ▪ Describe the importance of data privacy ▪ Describe the role of organization ▪ List data types and regulations ▪ List actions you can take
Data security	At the end of this short lesson, your students will be able to do the following: ▪ Describe data security ▪ Describe the data lifecycle ▪ List data types and risks ▪ List the risks of unsecured data ▪ List actions you can take
Email Security	At the end of this short lesson, your students will be able to do the following: ▪ Identify tactics used to compromise email security ▪ Understand why email is a target ▪ Recognize the signs of an email attack ▪ List actions to prevent email security compromise
Insider Threat	At the end of this short lesson, your students will be able to do the following: ▪ Describe the types of insider threat ▪ Understand how an insider event can occur ▪ List actions to avoid becoming or aiding an insider threat
Intellectual Property	At the end of this short lesson, your students will be able to do the following: ▪ Define intellectual property ▪ Identify how intellectual property theft can occur ▪ List actions that you can take to mitigate intellectual property theft

Module Name	Description
Intro to InfoSec	At the end of this short lesson, your students will be able to do the following: ▪ Describe information security awareness ▪ Describe key terms and concepts
Malware	At the end of this short lesson, your students will be able to do the following: ▪ Describe malware ▪ Describe types of malware ▪ Describe how to avoid malware ▪ List signs of a malware attack ▪ List actions you can take
Mobile Security	At the end of this short lesson, your students will be able to do the following: ▪ Describe how mobile devices are used in the workplace ▪ Understand the security risks involved with using mobile devices ▪ List actions for mitigating risks associated with using mobile devices
Multi-Factor Authentication	At the end of this short lesson, your students will be able to do the following: ▪ Describe the purpose of MFA ▪ List the types of MFA ▪ Describe how MFA increases security ▪ List actions you can take to secure your information
Password	At the end of this short lesson, your students will be able to do the following: ▪ Describe risks ▪ List characteristics of weak passwords ▪ List characteristics of strong and unique passwords ▪ List actions that protect your password
Phishing	At the end of this short lesson, your students will be able to do the following: ▪ Describe phishing and other common forms of cyberattacks ▪ Describe the risks associated with phishing attacks ▪ Describe how to spot and avoid phishing attacks ▪ List actions that employees can take to avoid becoming the victim of a phishing attack
Secure Travel	At the end of this short lesson, your students will be able to do the following: ▪ Identify how cybersecurity compromise can occur while traveling ▪ Describe the tactics that a bad actor can use ▪ Apply actions for staying safe while traveling
Social Engineering	At the end of this short lesson, your students will be able to do the following: ▪ Define social engineering ▪ Understand risks ▪ List typical attack vectors ▪ List actions you can take
Social Media	At the end of this short lesson, your students will be able to do the following: ▪ Describe the risks associated with social media ▪ Understand some of the common vulnerabilities associated with social media ▪ List actions that you can take to secure your social media accounts
Web Conference	At the end of this short lesson, your students will be able to do the following: ▪ Describe the risks associated with web conferences ▪ List actions you can take to mitigate the risks associated with web conferences

Module Name	Description
Working Remotely	At the end of this short lesson, your students will be able to do the following: ▪ Describe the risks associated with remote work ▪ Describe common strategies used by organizations to secure remote work environments ▪ List actions employees can take to keep their information secure while working remotely
Manager Awareness	At the end of this short lesson, your students will be able to do the following: ▪ Describe the evolution of cyber threats ▪ Describe the evolution of the attack surface ▪ Describe real-life case studies of high-profile cyber attacks ▪ List actions you can take to build a cyber-aware workforce
Manager Frameworks	At the end of this short lesson, your students will be able to do the following: ▪ Describe cyber security frameworks ▪ Describe the World Economic Forum (WEF) 10 Principles of Cyber Resilience ▪ Describe the NIST Cyber Security Framework (CSF) ▪ Describe where training fits in the NIST CSF Core ▪ Briefly describe the Fortinet Security Awareness Training Service
Manager Deployment	At the end of this short lesson, your students will be able to do the following: ▪ Describe how to plan the deployment of the Fortinet Security Awareness and Training service ▪ Describe how to deploy the service ▪ Describe how to perform a post-implementation and ongoing evaluation of the service

Communication Resources

Communication resources are available in both the Standard and Premium Service.

	Posters	Tip Sheets	Screensavers	Banners
Security Awareness and Training Service				✓
Be Aware: No Tailgating	✓		✓	
Lock Before You Leave	✓		✓	
See Something, Hear Something, Say Something	✓		✓	
Don't Be Too Quick To Click	✓		✓	
Free Wi-Fi Comes With a Price	✓		✓	
Be Unique: Your Login Credentials Are Keys for Cyber Criminals	✓		✓	
Insider Threats		✓		
Mobile Security		✓		

About the Fortinet Security Awareness and Training service

The Fortinet Security Awareness and Training service is a Software-as-a-Service (SaaS) offering that can be integrated with FortiPhish to provide a full turnkey solution. Training delivered in multiple formats, including video, text, audio, imagery, and animation, appeals to different learning styles to ensure that training is understood and applied. Smaller, more easily consumed lengths such as micro-learning and nano-learning coupled with communications resources allow organizations to augment their training to help reinforce key lessons.

Learn more about the service.

FORTINET®

www.fortinet.com

September 5, 2022 10:23 AM

1378653-A-0-EN