



**MÓDULOS DO CURSO**

# Serviço de Conscientização e Treinamento em Cibersegurança da Fortinet

## Módulos de formação de base

Os módulos de formação são módulos interativos de aproximadamente 8 minutos que visam ensinar através de apresentações e exercícios multimídia interativos. Nos cursos, também há questionários e avaliações.

	Serviço Padrão	Serviço Premium
Conscientização em segurança da informação	✓	✓
Criminosos	✓	✓
Engenharia social	✓	✓
Ataques de phishing	✓	✓
Segurança de e-mail	✓	✓
Malware e ransomware	✓	✓
Proteção por senha	✓	✓
Autenticação multifator		✓
Segurança de dados		✓
Privacidade de dados		✓
Controle de acesso		✓
Segurança móvel		✓
Ameaça interna		✓
Política sobre mesa limpa		✓
Trabalhando remotamente		✓
Segurança de conferência na web		✓
Comprometimento de e-mail comercial (BEC — Business Email Compromise)		✓
Propriedade intelectual		✓
Dicas para viagens seguras		✓
Redes sociais		✓
Gerentes: Estruturas de segurança da informação		✓
Gerentes: Conscientização em segurança da informação		✓
Gerentes: Implementação e gerenciamento do Serviço de Formação e Conscientização em Cibersegurança da Fortinet		✓



## Micromódulos de formação

Os micromódulos são um resumo dos módulos de base, que duram, normalmente, menos de 2 minutos cada, sendo usados como um seguimento dos módulos de base para reforçar um assunto em específico.

	Serviço Padrão	Serviço Premium
Engenharia social	✓	✓
Ataques de phishing	✓	✓
Segurança de e-mail	✓	✓
Malware e ransomware	✓	✓
Proteção por senha	✓	✓
Segurança de dados		✓
Privacidade de dados		✓
Comprometimento de e-mail comercial (BEC — Business Email Compromise)		✓
Ameaça interna		✓
Política sobre mesa limpa		✓

## Nanomódulos de formação

Os nanomódulos, que normalmente duram menos de 1 minuto, são utilizados para reforçar um assunto ou como suportes/ativos para promover a conscientização em Cibersegurança em toda a empresa.

	Serviço Padrão	Serviço Premium
Bisbilhoteiros	✓	✓
Tailgating	✓	✓
Viu algo, Ouviu algo, Diga algo	✓	✓
Siga a política da empresa	✓	✓
Evite redes Wi-Fi desconhecidas	✓	✓
Boa higiene de senha	✓	✓
Pense antes de clicar	✓	✓
Dicas para conferências na web		✓
Dicas para viagens		✓
Faça backup dos seus dados		✓
Descarte de dados		✓
Desative o Wi-Fi automático		✓
Criptografe dados confidenciais		✓
Ative os bloqueios de tela		✓
Atualize seu software		✓
Proteja seus dispositivos		✓
Sem localização por Bluetooth		✓
Usar autenticação multifator		✓

## Recursos de comunicação

	Conscientização InfoSec	Privacidade de dados	Segurança na Internet	Proteção por senha	Segurança física	
SERVIÇO PADRÃO	Conscientização em segurança da informação	✓				
	Criminosos	✓	✓			
	Engenharia social	✓		✓	✓	
	Ataques de phishing	✓	✓	✓	✓	
	Segurança de e-mail	✓	✓	✓		
	Malware e ransomware	✓		✓		
	Proteção por senha	✓	✓		✓	
	Autenticação multifator	✓	✓		✓	
	Segurança de dados	✓	✓	✓	✓	✓
	Privacidade de dados	✓	✓			
SERVIÇO PREMIUM	Controle de acesso	✓	✓		✓	
	Segurança móvel	✓		✓	✓	
	Ameaça interna	✓	✓	✓	✓	✓
	Política sobre mesa limpa	✓	✓			✓
	Trabalhando remotamente	✓	✓	✓		
	Segurança de conferência na web	✓		✓		
	Redes sociais	✓	✓	✓	✓	
	Comprometimento de e-mail comercial (BEC — Business Email Compromise)	✓	✓	✓	✓	
	Propriedade intelectual	✓	✓			
	Dicas para viagens seguras	✓		✓		✓
Gerentes: Estrutura de segurança da informação	✓	✓	✓			
Gerentes: Conscientização em segurança da informação	✓	✓				
Gerentes: Implementação do serviço	✓					

Os recursos de comunicação estão disponíveis nos serviços Padrão e Premium.

	Conscientização InfoSec	Privacidade de dados	Segurança na Internet	Proteção por senha	Segurança física	
SERVIÇO PADRÃO	Engenharia social	✓	✓		✓	
	Ataques de phishing	✓	✓	✓		
	Segurança de e-mail	✓	✓	✓		
	Malware e ransomware	✓		✓		
	Proteção por senha	✓	✓		✓	
	Segurança de dados	✓	✓	✓	✓	✓
	Privacidade de dados	✓	✓			
	Comprometimento de e-mail comercial (BEC — Business Email Compromise)	✓	✓		✓	
	Ameaça interna	✓	✓	✓	✓	✓
	Política sobre mesa limpa	✓	✓	✓		✓



## Descrições de cursos

Nome do módulo	Descrição
<b>Controle de acesso</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever o controle de acesso e estratégias Zero trust</li> <li>▪ Descrever a autenticação, autorização e auditoria</li> <li>▪ Listar os principais tipos de controle de acesso</li> <li>▪ Descrever a importância do controle de acesso</li> <li>▪ Listar ações a serem tomadas</li> </ul>
<b>Criminosos</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Identificar os tipos de criminosos</li> <li>▪ Entender os motivos dos criminosos</li> <li>▪ Relacionar ações para evitar o ataque de segurança cibernética</li> <li>▪ Entender as pessoas que são criminosas</li> </ul>
<b>Comprometimento de e-mail comercial</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descreve as estratégias comuns utilizadas por criminosos para comprometer a segurança do seu e-mail comercial</li> <li>▪ Identifica as diferentes fases de um ataque de BEC</li> <li>▪ Lista as ações que você pode adotar para se proteger de um ataque de BEC</li> </ul>
<b>Política sobre mesa limpa</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever os riscos</li> <li>▪ Definir o Princípio da mesa limpa</li> <li>▪ Listar os exemplos de adesão ao Princípio da mesa limpa</li> <li>▪ Relacionar as ações a serem executadas para proteger as informações em seu espaço de trabalho</li> </ul>
<b>Privacidade de dados</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever a privacidade dos dados</li> <li>▪ Descrever a importância da privacidade dos dados</li> <li>▪ Descrever o papel da organização</li> <li>▪ Listar tipos de dados e regulamentações</li> <li>▪ Listar ações que você pode tomar</li> </ul>
<b>Segurança de dados</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever a segurança dos dados</li> <li>▪ Descrever o ciclo de vida dos dados</li> <li>▪ Listar tipos de dados e riscos</li> <li>▪ Listar riscos dos dados desprotegidos</li> <li>▪ Listar ações que você pode tomar</li> </ul>
<b>Segurança de e-mail</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Identificar as táticas usadas para comprometer a segurança do e-mail</li> <li>▪ Entender por que o e-mail é um alvo</li> <li>▪ Reconhecer os sinais de um ataque por e-mail</li> <li>▪ Listar ações para evitar o comprometimento da segurança do e-mail</li> </ul>
<b>Ameaça interna</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever os tipos de ameaças internas</li> <li>▪ Entender como um evento interno pode ocorrer</li> <li>▪ Relacionar as ações para evitar se tornar ou ajudar uma ameaça interna</li> </ul>
<b>Propriedade intelectual</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Definição de propriedade intelectual</li> <li>▪ Identificar como pode ocorrer o roubo de propriedade intelectual</li> <li>▪ Lista do que você pode fazer para mitigar o roubo de propriedade intelectual</li> </ul>
<b>Introdução à InfoSec</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever a conscientização sobre segurança da informação</li> <li>▪ Descrever termos e conceitos principais</li> </ul>

Nome do módulo	Descrição
<b>Malware e ransomware</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever malware</li> <li>▪ Descrever os tipos de malware</li> <li>▪ Descrever como evitar o malware</li> <li>▪ Relacionar os sinais de um ataque de malware</li> <li>▪ Listar ações que você pode tomar</li> </ul>
<b>Segurança móvel</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever como os dispositivos móveis são usados no local de trabalho</li> <li>▪ Compreender os riscos de segurança envolvidos com o uso de dispositivos móveis</li> <li>▪ Relacionar as ações para mitigar os riscos associados ao uso de dispositivos móveis</li> </ul>
<b>Autenticação multifator</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descreva o propósito da MFA</li> <li>▪ Liste os tipos de MFA</li> <li>▪ Descreva como a MFA aumenta a segurança</li> <li>▪ Liste as ações que você pode adotar para proteger suas informações</li> </ul>
<b>Proteção por senha</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever os riscos</li> <li>▪ Listar características de senhas fracas</li> <li>▪ Listar características de senhas fortes e únicas</li> <li>▪ Listar ações que protegem sua sen</li> </ul>
<b>Ataques de phishing</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever phishing e outras formas comuns de ataques cibernéticos</li> <li>▪ Descrever os riscos associados aos ataques de phishing</li> <li>▪ Descrever como detectar e evitar ataques de phishing</li> <li>▪ Listar ações que os funcionários podem tomar para evitarem ser vítimas de um ataque de phishing</li> </ul>
<b>Dicas para viagens seguras</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Identificar como o comprometimento da segurança cibernética pode ocorrer durante a viagem</li> <li>▪ Descrever as táticas que um criminoso pode usar</li> <li>▪ Implementar ações para manter a segurança durante a viagem</li> </ul>
<b>Engenharia social</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Definir engenharia social</li> <li>▪ Compreender os riscos</li> <li>▪ Listar vetores de ataque típicos</li> <li>▪ Listar ações que você pode executar</li> </ul>
<b>Redes sociais</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever os riscos associados às redes sociais</li> <li>▪ Compreender algumas das vulnerabilidades comuns associadas às redes sociais</li> <li>▪ Liste as ações que você pode realizar para proteger suas contas de redes sociais</li> </ul>
<b>Segurança de conferência na web</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever os riscos associados a conferências na web</li> <li>▪ Listar as ações que você pode adotar para mitigar os riscos associados às conferências na web</li> </ul>
<b>Trabalhando remotamente</b>	<p>Ao final desta breve lição, seus estudantes poderão fazer o seguinte:</p> <ul style="list-style-type: none"> <li>▪ Descrever os riscos associados ao trabalho remoto</li> <li>▪ Descrever as estratégias comuns usadas pelas organizações para proteger ambientes de trabalho remotos</li> <li>▪ Listar ações que os funcionários podem realizar para manter suas informações seguras enquanto trabalham remotamente</li> </ul>

Nome do módulo	Descrição
<b>Gerentes: Estruturas de segurança da informação</b>	Ao final desta breve lição, seus estudantes poderão fazer o seguinte: <ul style="list-style-type: none"> <li>▪ Descrever a evolução das ameaças cibernéticas</li> <li>▪ Descrever a evolução da superfície de ataque</li> <li>▪ Descrever estudos de casos reais de ataques cibernéticos notáveis</li> <li>▪ Listar o que você pode fazer para desenvolver uma equipe consciente no ambiente cibernético</li> </ul>
<b>Gerentes: Conscientização em segurança da informação</b>	Ao final desta breve lição, seus estudantes poderão fazer o seguinte: <ul style="list-style-type: none"> <li>▪ Descrever as estruturas de segurança cibernética</li> <li>▪ Descrever os 10 princípios da resiliência cibernética do Fórum Econômico Mundial (FEM)</li> <li>▪ Descrever a estrutura de segurança cibernética NIST (CSF)</li> <li>▪ Descrever onde o treinamento entra no Núcleo do NIST CSF</li> <li>▪ Uma breve descrição do serviço de treinamento de conscientização de segurança da Fortinet</li> </ul>
<b>Gerentes: Implementação e gerenciamento do Serviço de Formação e Conscientização em Cibersegurança da Fortinet</b>	Ao final desta breve lição, seus estudantes poderão fazer o seguinte: <ul style="list-style-type: none"> <li>▪ Descrever como planejar a implantação do serviço de conscientização e treinamento de segurança da Fortinet</li> <li>▪ Descrever como implantar o serviço</li> <li>▪ Descrever como realizar uma pós-implantação e avaliação contínua do serviço</li> </ul>

## Recursos de comunicação

Os recursos de comunicação estão disponíveis tanto no serviço padrão como no premium.

	Cartazes	Folhas de sugestões	Proteções de ecrã	Banners
Serviço de formação e sensibilização para a segurança				✓
Esteja atento: não é permitido o acesso de pessoas não autorizadas	✓		✓	
Bloqueie sempre o ecrã antes de sair	✓		✓	
Viu alguma coisa, ouviu alguma coisa, diga alguma coisa	✓		✓	
Pense duas vezes antes de clicar	✓		✓	
O Wi-Fi gratuito afinal sai caro	✓		✓	
Seja criativo: as suas credenciais de início de sessão são chaves de acesso para os cibercriminosos	✓		✓	
Ameaças internas		✓		
Segurança móvel		✓		

## Acerca do serviço de formação e sensibilização para a segurança da Fortinet

O serviço de formação e sensibilização para a segurança da Fortinet é uma oferta de software disponibilizado como um serviço (SaaS) que pode ser integrada com o FortiPhish para fornecer uma solução chave na mão completa. A formação disponibilizada em vários formatos, incluindo vídeo, texto, áudio, imagens e animação, apela a diferentes estilos de aprendizagem para assegurar que a formação é compreendida e aplicada. Durações mais curtas e mais facilmente consumidas, tais como micro-aprendizagem e nano-aprendizagem, juntamente com recursos de comunicação, permitem às organizações aumentar a sua formação para ajudar a reforçar as lições mais importantes.

[Saber mais sobre o serviço.](#)



www.fortinet.com