L'AKADÉMIE DU DIGITAL · PROGRAMA DE FORMAÇÃO Certificação Qualiopi em preparação

Engenharia Social e Phishing

FOR-CYBER-M4-A · Cibersegurança e Conformidade

Compreender e desmontar as manipulações humanas da ciberfraude

DURAÇÃO
7 h

PREÇO
450 € s/ IVA

PÚBLICO
Empresas e particulares

PRAZO DE ACESSO
Acesso em 2 dias úteis após validação da necessidade e dos pré-requisitos.

Preços indicados «a partir de», excluindo orçamento específico e promoções. Preços sem IVA, a partir de 2 participantes. IVA a 20 %.

Objetivos pedagógicos

- Compreender os mecanismos psicológicos da engenharia social (alavancas de influência e de manipulação)
- Identificar as principais técnicas de ataque: phishing, spear phishing, vishing, smishing, usurpação, pretexting
- Identificar os sinais de alerta de uma mensagem ou de uma solicitação fraudulenta
- Reagir corretamente perante uma tentativa e saber comunicar um incidente
- Sensibilizar e treinar o seu círculo ou a sua equipa (campanhas de simulação)
- Adotar reflexos duradouros de vigilância digital

Público-alvo

- Qualquer colaborador, seja qual for o seu nível técnico
- Funções expostas: receção, administrativo, contabilidade/finanças, RH, comercial, direção
- Responsáveis de segurança e gestores que queiram sensibilizar as suas equipas

Pré-requisitos

- Saber utilizar um computador ou um smartphone e o correio eletrónico.
- Utilizar regularmente ferramentas digitais do dia a dia.
- Ter uma sensibilização de base para a cibersegurança (módulo Iniciação aconselhado).
- Ter motivação para reforçar a sua vigilância e a da sua equipa.

Programa

TEORIA Módulo Teórico — Compreender a engenharia social

Este módulo explica o que é a engenharia social e porque é que o ser humano é o elo visado, decifrando as alavancas psicológicas exploradas (autoridade, urgência, medo, curiosidade, ganância, reciprocidade, prova social). Apresenta um panorama das técnicas (phishing, spear phishing, vishing, smishing, usurpação de identidade, pretexting, burla do presidente, fraude do falso fornecedor), detalha a anatomia de um ataque de phishing, os sinais de alerta e os reflexos a adotar em caso de dúvida ou de incidente (comunicação interna, Cybermalveillance.gouv.fr).

Objetivo : compreender os mecanismos da engenharia social e saber identificar as tentativas de manipulação para melhor se proteger.

- Decifração das alavancas psicológicas da manipulação.
- Panorama completo e concreto das técnicas de ataque.
- Sinais de alerta e reflexos de comunicação, com uma finalidade defensiva.

Avaliação : Questionário de escolha múltipla sobre as técnicas e as alavancas psicológicas, exercício de identificação de sinais de alerta.

Acolhimento e apresentação	15 min	Apresentar o programa, os objetivos e o quadro ético/defensivo. Apresentação oral, suporte visual (diapositivos), ronda de apresentações.	
O que é a engenharia social?	35 min	O ser humano como elo visado; porque é que os ataques funcionam. Exposição interativa, exemplos, debate.	Perguntas orais de compreensão.
Alavancas psicológicas	45 min	Autoridade, urgência, medo, curiosidade, ganância, reciprocidade, prova social. Exposição, análise de casos, discussão.	Questionário de escolha múltipla sobre as alavancas.
Panorama das técnicas	1h00	Phishing, spear phishing, vishing, smishing, usurpação, pretexting, burla do presidente. Exposição ilustrada, exemplos reais, anatomia de um ataque.	Exercício de identificação de sinais de alerta.
Reagir e comunicar	40 min	Sinais de alerta (remetente, ligações, anexos); reflexos e comunicação. Exposição, lista de verificação, recursos (Cybermalveillance).	Questionário intermédio de escolha múltipla.
Síntese	10 min	Resumir os pontos-chave e preparar a oficina. Resumo, feedback dos participantes.	Questionário rápido de escolha múltipla no final do módulo.

OFICINA Oficina Prática — Detetar, reagir e sensibilizar

Os participantes analisam uma coleção de falsas mensagens (e-mails, SMS, cenários de chamada) e identificam coletivamente os indícios, colocam-se em situação perante um cenário de ataque (jogo de papéis, tomada de decisão), constroem uma ficha de reflexos «identificar e reagir» e concebem as linhas gerais de uma minicampanha de sensibilização (mensagens-chave, simulação de phishing ético e enquadrado).

Objetivo : saber detetar uma tentativa, reagir corretamente e sensibilizar o seu círculo ou a sua equipa.

- Análise de casos reais variados (e-mail, SMS, chamada).
- Simulação por jogo de papéis e tomada de decisão.
- Produção de uma ficha de reflexos diretamente utilizável.
- Conceção de uma minicampanha de sensibilização ética.

Avaliação : produção dos entregáveis (análise de casos, ficha de reflexos, plano de sensibilização), apresentação oral curta e revisão coletiva.

Início da oficina	15 min	Apresentar o objetivo e o quadro ético das simulações. Apresentação, lembrete do quadro (sem dados reais), grupos.	
Análise de falsas mensagens	55 min	Analisar e-mails, SMS e cenários de chamada; identificar os indícios. Estudo de caso guiado, identificação coletiva, grelha de análise.	Entregável: análise de casos.
Simulação	50 min	Reagir perante um cenário de ataque (jogo de papéis, decisão). Jogo de papéis, debriefing coletivo, boas reações.	Observação; participação no jogo de papéis.
Ficha de reflexos	40 min	Construir uma ficha de reflexos «identificar e reagir». Trabalho prático, modelo de ficha de reflexos, acompanhamento.	Entregável: ficha de reflexos.
Campanha de sensibilização	30 min	Conceber uma minicampanha (mensagens-chave, simulação ética); apresentar. Modelo de campanha, apresentações curtas, feedback.	Avaliação sumativa: plano de sensibilização + questionário final de escolha múltipla.
Inquérito de satisfação	10 min	Recolher a satisfação a quente. Questionário de satisfação.	Inquérito de satisfação.

Modalidades e meios pedagógicos

Formação presencial nas nossas instalações ou nas suas, em grupo reduzido. Alternância de contributos teóricos, oficinas práticas e simulações.

Material necessário :

8 GB de RAM

Modalidades de avaliação

Avaliação das aprendizagens durante e no final da formação; certificado de conclusão entregue a cada formando.

Acessibilidade

Formação acessível a pessoas com deficiência. Contacte-nos antes da inscrição para estudarmos as adaptações necessárias.

Financiamento

Orçamento ou convenção de formação a pedido. A certificação Qualiopi está em preparação: a elegibilidade para financiamentos OPCO será aberta após a sua obtenção.

Auditoria de certificação prevista para T1 2027. Sem elegibilidade OPCO antes da sua obtenção.