Digital e inteligência artificial

Sensibilização para a cibersegurança

Meio dia para que cada colaborador reconheça os ataques mais comuns e saiba o que fazer: e-mail de phishing, falso telefonema de um dirigente, pedido fraudulento de alteração de dados bancários, pen USB armadilhada, ransomware. Os exemplos são tirados de situações de empresa, os bons reflexos mantêm-se simples e a sessão termina com o procedimento de comunicação de incidentes da sua empresa.

Duração : 0,5 dia

Objetivos

1. Reconhecer um e-mail, uma mensagem ou um telefonema fraudulento
2. Aplicar as regras de base: palavras-passe robustas, gestor de palavras-passe, autenticação de dois fatores
3. Explicar como um ransomware entra na empresa e o que limita os danos
4. Proteger as informações da empresa em deslocação, em teletrabalho e nas redes sociais
5. Comunicar sem demora um incidente ou uma dúvida, segundo o procedimento interno

Programa

Meio dia

• Porque os atacantes visam os colaboradores: phishing, usurpação de identidade, fraude do presidente, falsa alteração de IBAN

• Exercício: detetar os indícios numa série de e-mails verdadeiros e falsos

• Palavras-passe, autenticação de dois fatores, atualizações, pens USB e dispositivos pessoais

• Assistentes de IA e fugas de informação: o que nunca se deve copiar para uma ferramenta online

• Reflexos em caso de dúvida ou de incidente, procedimento de comunicação da empresa, quiz final

Metodologia

• Exemplos reconstituídos de e-mails e mensagens fraudulentos

• Quiz interativo ao longo da sessão

• Jogo de papéis: o telefonema insistente de um falso fornecedor que pede para alterar os seus dados bancários

• Animação possível em francês ou em darija para as equipas de terreno

• Ficha de reflexos de uma página entregue a cada participante

Avaliação e documentos

Quiz final de aquisições e avaliação a quente em D+1. Certificado numerado, verificável online, para cada participante; relatório de formação entregue à empresa, com as perguntas que levantaram mais dificuldades.

Materiais bilingues para cada participante; cada formação presencial inclui o seu gémeo digital no OmniLearn.

Bom saber

Formato curto, que pode ser programado para vários grupos sucessivos, incluindo as equipas por turnos. Para as regras sobre dados pessoais, veja «Dados pessoais: Lei 09-08 e CNDP».

Informações práticas

Duração	0,5 dia
Público	Todos os colaboradores que utilizam um computador, correio eletrónico ou um telemóvel profissional
Pré-requisitos	Nenhum pré-requisito
Número de participantes	Grupos de 6 a 12 participantes, na empresa
Formato	Na empresa, presencial nas suas instalações
Língua	Francês, darija ou inglês; materiais bilingues
Financiamento	Contratos especiais de formação da OFPPT (TFP), GIAC, Maroc PME: preparamos os processos consigo, sem custo adicional.
Personalização do programa	Programa adaptado aos seus procedimentos, aos seus equipamentos e ao seu público

Perguntas frequentes

São precisos conhecimentos de informática?
Não. A sessão destina-se a qualquer colaborador que utilize correio eletrónico, um computador ou um telemóvel profissional. Nenhum termo técnico é empregue sem ser explicado por um exemplo.

A formação substitui as proteções técnicas?
Não, completa-as. Antivírus, filtragem e cópias de segurança reduzem os riscos, mas grande parte dos ataques passa por um colaborador que clica, responde ou reencaminha. A sessão atua sobre esse elo.

Qual é a diferença para a formação ISO/IEC 27001:2022?
A ISO/IEC 27001:2022 destina-se às pessoas que constroem ou auditam um sistema de gestão da segurança da informação. Este meio dia visa todos os colaboradores e incide sobre os bons reflexos do dia a dia.