Cofinanciado pela
União Europeia

FinPower

Módulo 6: SEGURANÇA ONLINE,

COMPRAS ONLINE E MÉTODOS DE PAGAMENTO ALTERNATIVOS

Preparado por: RightChallenge

NÚMERO DE IDENTIFICAÇÃO DO PROJETO:

2022-1-AT01-KA220-ADU-000087985

Índice

OBJETIVOS DE APRENDIZAGEM

Os objetivos de aprendizagem deste módulo são diversos e concebidos para dotar os participantes de conhecimentos abrangentes e competências práticas em áreas específicas.

O primeiro tópico é "Segurança online". Aprofunda o domínio da segurança online, destacando riscos comuns como o roubo de identidade, transações fraudulentas e ameaças à cibersegurança. Explica os impactos financeiros e emocionais destes riscos para os indivíduos, realçando a importância de salvaguardar as informações pessoais.

O segundo tópico é "Como comprar online com segurança". Os objetivos principais incluem a compreensão dos riscos associados às compras online, a identificação dos métodos comuns de fraude e cibercrime online, a avaliação da segurança dos sítios Web e dos métodos de pagamento e a implementação de estratégias para proteger as informações pessoais e financeiras. Os formandos também serão treinados para reconhecer potenciais fraudes online para melhorar a proteção pessoal e dos pares.

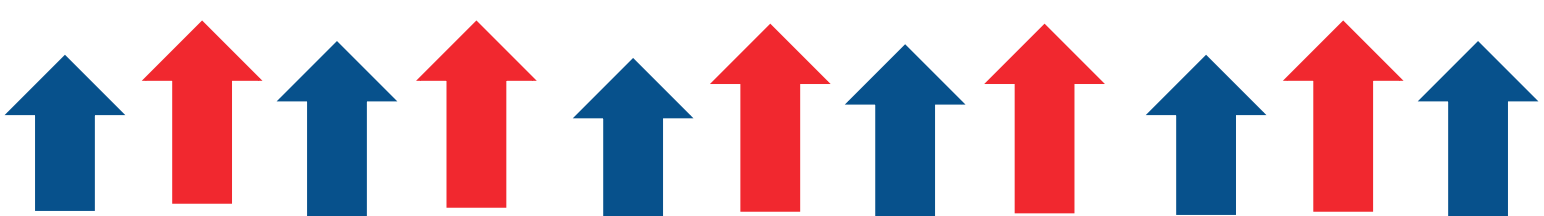
Por último, o tema "Quais são os métodos de pagamento alternativos?" centra-se na compreensão, análise e utilização segura de vários métodos de pagamento alternativos, como as carteiras eletrónicas, as criptomoedas e os pagamentos móveis. Também enfatiza a educação dos participantes, especialmente das mulheres, sobre métodos de pagamento sustentáveis, capacitando-os a fazer escolhas financeiras ambiental e socialmente responsáveis.

De um modo geral, estes objetivos de aprendizagem visam proporcionar aos participantes uma compreensão abrangente de cada tópico e dotá-los dos conhecimentos e competências necessários para navegarem eficazmente no assunto.

SEGURANÇA ONLINE

Identificação de riscos comuns de segurança

De acordo com o FBI, conforme citado pela Kaspersky, **o roubo de identidade** ocorre quando alguém obtém e utiliza ilegalmente as informações pessoais de outra pessoa (como o nome,



o número da Segurança Social, o número do cartão de crédito ou os detalhes da conta bancária) para cometer fraudes ou outros crimes.

Exemplos:

Utilização não autorizada das informações do cartão de crédito ou da conta bancária de alguém para efetuar compras.

Abrir novas contas de crédito ou empréstimos utilizando a identidade de outra pessoa.

Preenchimento de declarações fiscais fraudulentas utilizando números da Segurança Social roubados.

As transações fraudulentas envolvem a aquisição, utilização ou transferência não autorizada ou fraudulenta de fundos, bens ou outros ativos através de meios enganosos ou desonestos.

Exemplos:

Um burlão que se faz passar por representante de uma empresa legítima e solicita o pagamento de serviços ou produtos falsos.

Acesso não autorizado a uma conta bancária ou cartão de crédito para efetuar levantamentos ou compras não autorizadas.

Falsa faturação ou esquemas de faturação em que são enviadas faturas por serviços nunca prestados.

As ameaças à cibersegurança referem-se a quaisquer atividades ou eventos maliciosos que procuram comprometer a confidencialidade, a integridade ou a disponibilidade de informações e sistemas digitais.

Exemplos:

Ataques de malware (por exemplo, vírus, ransomware, spyware) que infectam e comprometem sistemas ou redes informáticas.

E-mails de phishing ou esquemas de engenharia social concebidos para enganar as pessoas, levando-as a revelar informações sensíveis ou a clicar em ligações maliciosas.

Violações de dados em que partes não autorizadas obtêm acesso a informações sensíveis armazenadas em bases de dados ou servidores.

Como é que estes riscos podem ter um impacto financeiro e emocional nos indivíduos?

Impacto financeiro:

Roubo de identidade: As vítimas de roubo de identidade podem sofrer perdas financeiras devido a transações não autorizadas, empréstimos fraudulentos ou encargos nas suas contas. Podem também incorrer em despesas relacionadas com serviços de resolução de roubo de identidade e honorários legais.

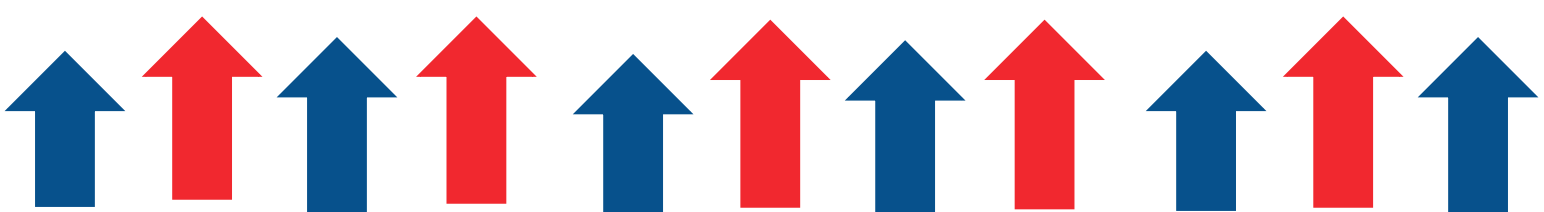
Transações fraudulentas: As pessoas afetadas por transações fraudulentas podem sofrer perdas financeiras diretas se os fundos forem roubados ou se forem feitas cobranças não autorizadas nas suas contas. Podem também sofrer impactos financeiros indiretos, como taxas por descobertos ou cheques devolvidos.

Ameaças à cibersegurança: As vítimas de ameaças à cibersegurança podem sofrer perdas financeiras resultantes do roubo de informações financeiras, do pagamento de resgates para recuperar o acesso a dados encriptados ou dos custos associados à recuperação de violações de dados (por exemplo, investigações forenses, multas regulamentares, indemnização de clientes).

Impacto emocional:

Roubo de identidade: O impacto emocional do roubo de identidade pode ser significativo, causando sentimentos de violação, ansiedade e impotência. As vítimas podem sentir stress e frustração enquanto navegam no processo de denúncia do roubo, contestação de cobranças fraudulentas e recuperação da sua identidade.

Transações fraudulentas: As pessoas afetadas por transações fraudulentas podem sentir-se traídas e vulneráveis, especialmente se a fraude envolver alguém em quem confiavam. Podem também sentir uma perda de controlo sobre a sua segurança financeira e privacidade.



Ameaças à cibersegurança: As vítimas de ameaças à cibersegurança podem sentir medo, ansiedade e desconfiança quanto à segurança das suas informações pessoais e atividades online. Podem também sentir uma sensação de vulnerabilidade e frustração com a perceção de falta de controlo sobre a sua privacidade e segurança digitais.

Atividade: Discussão em grupo sobre as recentes violações de segurança e o seu impacto nos indivíduos e nas organizações.

Esta atividade tem como objetivo analisar e discutir as recentes violações de segurança e o seu impacto nos indivíduos e nas organizações, incluindo as consequências financeiras e emocionais, as lições aprendidas e as estratégias de prevenção.

Passo a passo:

1. Dividir os participantes em pequenos grupos de 4-6 elementos.

2. Atribua a cada grupo um estudo de caso de violação de segurança recente ou um artigo de notícias para analisar. Os exemplos incluem violações de dados em grandes empresas, ataques de ransomware a organizações de cuidados de saúde ou esquemas de phishing dirigidos a indivíduos.

Podem ser utilizados os seguintes exemplos:

<u>Violações de dados em grandes empresas:</u>

Violação de dados do CAM4 (março de 2020): O site de streaming de vídeos para adultos CAM4 teve o seu servidor Elasticsearch violado, expondo mais de 10 mil milhões de registos. Os registos violados incluíam nomes completos, endereços de e-mail, orientação sexual, transcrições de chat, transcrições de correspondência por e-mail, hashes de palavra-passe, endereços IP e registos de pagamento.

Violação de dados do Yahoo (outubro de 2017): A Yahoo revelou que uma violação em agosto de 2013 tinha comprometido 3 mil milhões de contas. A violação foi comunicada pela primeira vez pela Yahoo quando estava a negociar a sua venda à Verizon.

Violação dos dados Aadhaar (março de 2018): Os dados pessoais de mais de mil milhões de cidadãos indianos armazenados na maior base de dados biométricos do mundo podem ser comprados online.

Ataques de ransomware a organizações de cuidados de saúde:

Centro Médico da Universidade de Vermont (UVM) (outubro de 2020): Os funcionários do Centro Médico da UVM não puderam utilizar os registos de saúde eletrónicos (EHR), os programas de pagamentos e outras ferramentas digitais vitais durante quase um mês. Muitas cirurgias tiveram de ser remarcadas e os doentes com cancro tiveram de se deslocar a outro local para receberem tratamento por radiação.

Sistema de saúde Inova: O Inova Health System foi um dos prestadores de cuidados de saúde que foi vítima de um ataque de ransomware.

Phishing Scams dirigidos a pessoas singulares:

Spear Phishing: Este é um método de phishing direcionado que os cibercriminosos utilizam para roubar as suas informações fazendo-se passar por uma fonte de confiança.

Phishing HTTPS: Um cibercriminoso engana-o para que forneça as suas informações pessoais utilizando um sítio Web malicioso.

Phishing de correio eletrónico: Um dos ataques de phishing mais comuns é o phishing de correio eletrónico. O phishing de correio eletrónico é quando um ciberataque lhe envia uma mensagem de correio eletrónico fingindo ser outra pessoa, na esperança de que responda com as informações solicitadas.

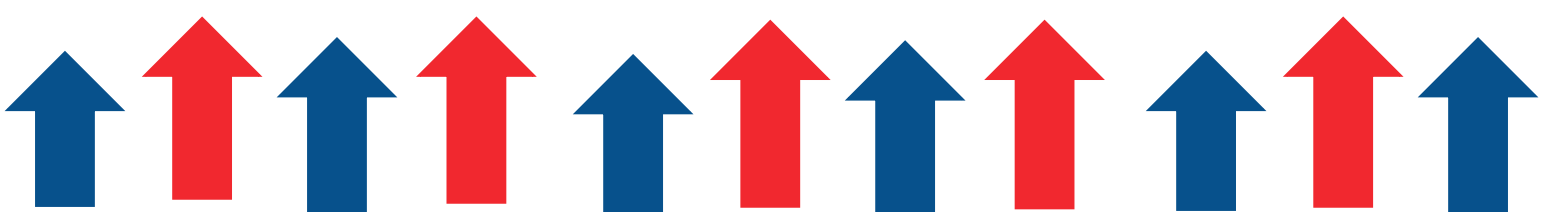
3. Forneça aos grupos perguntas orientadoras para facilitar o debate:

- Quais foram as circunstâncias e o âmbito da violação de segurança?

- Como é que a violação teve impacto financeiro e emocional nos indivíduos e nas organizações?

- Quais foram as principais lições aprendidas com o incidente?

- Que estratégias ou medidas poderiam ter sido aplicadas para evitar a infração?



4. dê aos grupos 20-30 minutos para reverem o estudo de caso ou o artigo, discutirem as questões e prepararem os pontos-chave para a apresentação.

5 - Após o tempo de discussão, reúnam-se novamente em grupo.

6. cada grupo apresenta um resumo das suas conclusões, destacando os principais aspetos da violação de segurança, o seu impacto, as lições aprendidas e as medidas preventivas.

7. incentivar o debate aberto e a troca de ideias entre os participantes.

8. Facilitar uma sessão de balanço em que os participantes refletem sobre temas comuns, desafios e melhores práticas discutidos nos estudos de caso.

9. concluir a atividade resumindo as principais conclusões e salientando a importância da sensibilização para a cibersegurança e das medidas proactivas para atenuar os riscos de segurança.

A importância das medidas de segurança

Antes de nos debruçarmos sobre os meandros da segurança online, vamos parar um pouco para perceber porque é que a proteção das informações pessoais é tão vital. As informações pessoais, desde o seu nome aos seus dados financeiros, desempenham um papel crucial nas nossas vidas.

Abrange uma vasta gama de dados que podem ser utilizados para identificar ou localizar uma pessoa. Isto inclui, mas não se limita a:

- Nome
- Endereço
- Número de Segurança Social (SSN)
- Data de nascimento
- Endereço de correio eletrónico.
- Número de telefone.
- Informações financeiras (por exemplo, números de cartões de crédito, detalhes de contas bancárias)

- Informações médicas
- Credenciais de contas online (por exemplo, nomes de utilizador, palavras-passe)

A proteção destas informações é fundamental pelas seguintes razões

Roubo de identidade: Um dos riscos mais significativos associados ao facto de as informações pessoais caírem nas mãos erradas é o roubo de identidade. Os ladrões de identidade podem utilizar informações pessoais roubadas para abrir contas fraudulentas, efetuar compras não autorizadas ou mesmo cometer crimes em nome da vítima. O custo financeiro e emocional do roubo de identidade pode ser substancial, uma vez que as vítimas gastam frequentemente muito tempo e recursos para retificar os danos causados ao seu crédito e reputação.

Fraude financeira: As informações pessoais são frequentemente visadas por cibercriminosos que procuram cometer fraudes financeiras. Isto pode envolver acesso não autorizado a contas bancárias, fraude com cartões de crédito ou pedidos de empréstimo fraudulentos utilizando identidades roubadas. As perdas financeiras resultantes deste tipo de fraude podem ser devastadoras, afetando a pontuação de crédito dos indivíduos, a estabilidade financeira e a confiança nas instituições financeiras.

Violações de privacidade: A salvaguarda das informações pessoais é essencial para proteger os direitos de privacidade dos indivíduos. O acesso não autorizado a dados pessoais pode resultar em violações de privacidade, em que informações sensíveis são expostas a partes não autorizadas. As violações de privacidade podem levar a constrangimentos, danos à reputação e erosão da confiança nas organizações responsáveis pela proteção dos dados pessoais.

Consequências legais e regulamentares: As organizações que não protegem adequadamente as informações pessoais podem enfrentar consequências legais e regulamentares. As leis de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) na Europa ou a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos, impõem requisitos rigorosos para a recolha, armazenamento e tratamento de dados pessoais. O não cumprimento desses regulamentos pode resultar em multas significativas, responsabilidades legais e danos à reputação de uma organização.

Melhores práticas para a proteção de informações pessoais

Para garantir a segurança das suas informações pessoais, siga estes passos essenciais:

Utilizar palavras-passe fortes: Crie palavras-passe fortes e únicas para cada conta online e altere-as regularmente. Evite utilizar palavras-passe fáceis de adivinhar ou reutilizar palavras-passe em várias contas.

Ativar a autenticação de dois fatores (2FA): Sempre que possível, ative a autenticação de dois fatores para adicionar uma camada extra de segurança às suas contas online. A 2FA exige que os utilizadores forneçam uma segunda forma de verificação, como um código enviado para o seu dispositivo móvel, para além da sua palavra-passe.

Seja cauteloso com as informações pessoais: Tenha cuidado ao partilhar informações pessoais online ou por telefone. Evite fornecer informações sensíveis, a menos que seja necessário, e verifique a legitimidade dos pedidos antes de partilhar quaisquer dados.

Proteja os seus dispositivos: Mantenha os seus dispositivos, incluindo computadores, smartphones e tablets, seguros, instalando software antivírus, ativando firewalls e mantendo o software atualizado com os patches de segurança mais recentes.

Eduque-se: Mantenha-se informado sobre as táticas comuns de burla e phishing utilizadas pelos cibercriminosos para enganar as pessoas e levá-las a revelar informações pessoais. Seja vigilante e cético em relação a e-mails, telefonemas ou mensagens não solicitados que peçam informações pessoais ou pagamentos.

Visão geral da segurança das contas e transações online para evitar o acesso não autorizado

Na era digital atual, a segurança das contas e transações online é de extrema importância para proteger as informações pessoais e financeiras sensíveis contra o acesso não autorizado e atividades fraudulentas. A segurança de contas e transações online envolve a implementação de uma combinação de medidas preventivas e práticas recomendadas para proteger contra várias ameaças de cibersegurança, como pirataria informática, phishing e roubo de identidade. Abaixo estão os principais componentes da segurança de contas e transações online:

Palavras-passe fortes:

- Utilize palavras-passe fortes e únicas para cada conta online.
- Evite utilizar palavras-passe fáceis de adivinhar, como "password123" ou "123456".
- Considere a utilização de uma frase-passe composta por uma combinação de letras, números e caracteres especiais.
- Atualize regularmente as palavras-passe e evite reutilizá-las em várias contas.

Autenticação de dois fatores (2FA):

- Ativar a autenticação de dois fatores (2FA) sempre que disponível.
- A 2FA acrescenta uma camada extra de segurança ao exigir que os utilizadores forneçam uma segunda forma de verificação, como um código enviado para o seu dispositivo móvel, para além da sua palavra-passe.
- Isto ajuda a evitar o acesso não autorizado, mesmo que uma palavra-passe seja comprometida.

Comunicação segura:

- Assegurar que as transações e comunicações online são efetuadas através de canais seguros.
- Procure HTTPS no URL do sítio Web e um ícone de cadeado na barra de endereço do navegador, indicando que a ligação está encriptada.
- Evite transmitir informações sensíveis através de redes Wi-Fi não seguras, uma vez que estas podem ser vulneráveis à interceção por parte de atacantes.

Atualizações regulares de software:

- Manter o software, os sistemas operativos e as aplicações atualizados com os patches de segurança e as atualizações mais recentes.
- As vulnerabilidades em software desatualizado podem ser exploradas por atacantes para obter acesso não autorizado a dispositivos e contas.

Cuidado com os ataques de phishing:

- Tenha cuidado com e-mails, mensagens de texto ou chamadas telefónicas de phishing que tentam enganar os utilizadores para que revelem informações pessoais ou cliquem em ligações maliciosas.
- Evite clicar em ligações ou descarregar anexos de mensagens de correio eletrónico suspeitas ou não solicitadas.
- Verificar a legitimidade dos pedidos de informações pessoais antes de fornecer quaisquer dados sensíveis.

Utilizar métodos de pagamento seguros:

- Ao efetuar transações online, utilize métodos de pagamento seguros, como cartões de crédito ou plataformas de pagamento respeitáveis que ofereçam proteção ao comprador.
- Evite fornecer informações de pagamento a sítios Web não seguros ou desconhecidos.

Monitorizar a atividade da conta:

- Monitorizar regularmente a atividade da conta e os extratos para detetar quaisquer transações não autorizadas ou atividades suspeitas.
- Comunicar imediatamente quaisquer transações não autorizadas ou atividades suspeitas à respetiva instituição financeira ou prestador de serviços.

Encriptação de dados:

- Utilizar tecnologias de encriptação para proteger dados sensíveis, tanto em trânsito como em repouso.
- A encriptação codifica os dados para os tornar ilegíveis para utilizadores não autorizados, protegendo-os assim contra interceção ou roubo.

Explicação sobre como reconhecer e evitar fraudes para se proteger de perdas financeiras

As burlas assumem várias formas e podem visar indivíduos através de diferentes canais, incluindo e-mails, chamadas telefónicas, mensagens de texto e anúncios online. Reconhecer e evitar as burlas é essencial para se proteger de perdas financeiras e outras consequências

adversas. Segue-se uma explicação das principais estratégias para reconhecer e evitar burlas:

Educar-se a si próprio:

- Mantenha-se informado sobre os tipos mais comuns de burlas e esquemas fraudulentos, como as burlas de phishing, as burlas de investimento e as burlas de lotaria.
- Esteja atento às táticas mais recentes utilizadas pelos burlões para enganar as pessoas e explorar a sua confiança.

Seja cético em relação a comunicações não solicitadas:

- Tenha cuidado com e-mails, chamadas telefónicas ou mensagens de texto não solicitadas que peçam informações pessoais ou financeiras.
- Evite responder ou clicar em ligações em comunicações não solicitadas, especialmente se parecerem suspeitas ou demasiado boas para serem verdadeiras.

Verificar a legitimidade dos pedidos:

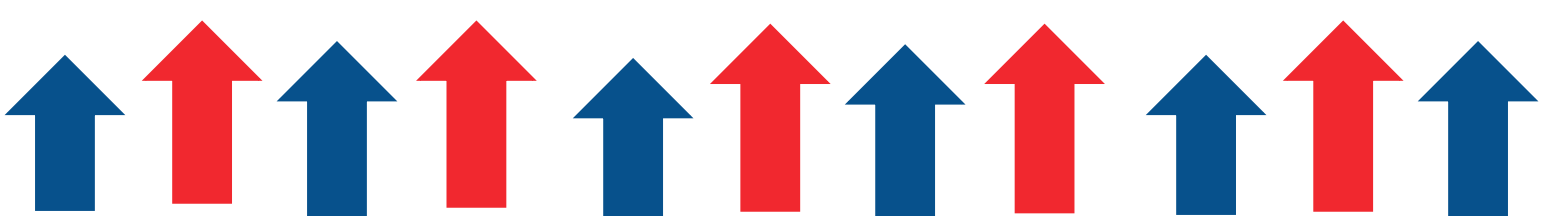
- Verificar a legitimidade dos pedidos de informações pessoais ou financeiras antes de fornecer quaisquer dados sensíveis.
- Contactar diretamente a organização utilizando as informações de contacto oficiais para confirmar a autenticidade dos pedidos.

Evitar tomar decisões precipitadas:

- Evite tomar decisões precipitadas ou agir impulsivamente em resposta às táticas de pressão utilizadas pelos burlões.
- Reserve algum tempo para pesquisar e verificar as ofertas ou oportunidades antes de assumir qualquer compromisso financeiro.

Proteger as informações pessoais:

- Proteger as informações pessoais e financeiras, evitando a partilha de dados sensíveis com partes desconhecidas ou não verificadas.



- Tenha cuidado ao fornecer informações pessoais online, especialmente em sítios Web que não sejam seguros ou fiáveis.

Confie nos seus instintos:

- Confie nos seus instintos e desconfie de ofertas ou oportunidades que pareçam demasiado boas para serem verdadeiras.
- Se algo parecer suspeito ou não parecer correto, tome as precauções necessárias e procure aconselhamento junto de fontes de confiança.

Atividade: Cenário de dramatização em que os alunos representam a segurança das suas contas e transações online.

O objetivo desta atividade de encenação é envolver os participantes num cenário simulado em que atuam para proteger as suas contas e transações online. Ao participarem ativamente no exercício de dramatização, os participantes ganharão experiência prática na implementação de medidas de segurança para evitar o acesso não autorizado às suas contas e transações online.

Materiais necessários:

- Propostas de cenários de role-playing (preparadas com antecedência)
- Adereços (opcional)
- Materiais de escrita

Instruções:

Introdução (5 minutos):

Introduza o objetivo da atividade de dramatização: praticar a segurança de contas e transações online para evitar o acesso não autorizado.

Explique que os participantes serão divididos em pares ou pequenos grupos para representarem diferentes cenários relacionados com a segurança online.

Atribuição de cenários (5 minutos):

Divida os participantes em pares ou pequenos grupos.

Atribua a cada par/grupo um cenário específico de dramatização relacionado com a segurança de contas e transações online. Os cenários podem incluir:

Criar uma palavra-passe forte e ativar a autenticação de dois fatores para uma conta de correio eletrónico.

Atualização das definições de segurança de uma conta bancária online.

Reconhecer e evitar tentativas de phishing numa mensagem de correio eletrónico ou de texto.

Verificar a legitimidade de um sítio de compras online antes de efetuar uma compra.

Preparação para o jogo de papéis (10 minutos):

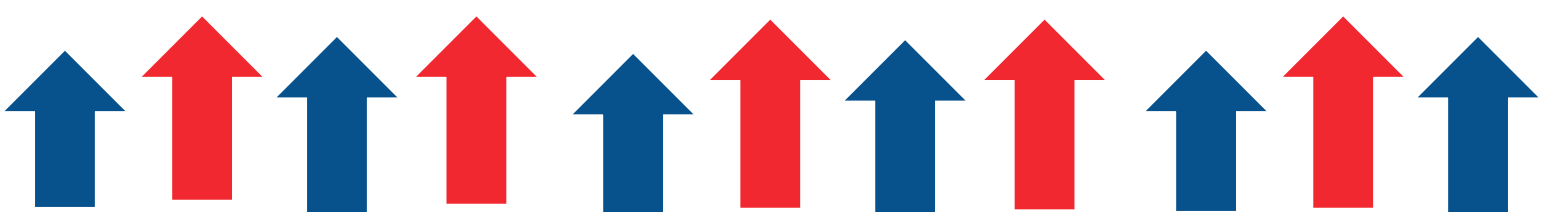
Dê aos participantes uma breve panorâmica do cenário que lhes foi atribuído, incluindo os objetivos que devem atingir e as ações específicas que devem tomar.

Breve descrição geral:

a) Criar uma palavra-passe forte e ativar a autenticação de dois fatores para uma conta de correio eletrónico: Os participantes simularão o processo de criação de uma palavra-passe forte e de ativação da autenticação de dois fatores para aumentar a segurança de uma conta de correio eletrónico. Discutirão estratégias para criar uma senha segura e implementar medidas de autenticação adicionais para impedir o acesso não autorizado.

b) Atualização das definições de segurança de uma conta bancária online: Os participantes irão dramatizar as etapas envolvidas na atualização das definições de segurança de uma conta bancária online. Reverão e ajustarão as definições de privacidade, definirão alertas para atividades suspeitas e explorarão outras características de segurança oferecidas pela plataforma bancária online.

c) Reconhecer e evitar tentativas de phishing num e-mail ou mensagem de texto: Os participantes simularão uma tentativa de phishing num e-mail ou mensagem de texto e praticarão o reconhecimento dos sinais de alerta de uma comunicação fraudulenta. Discutirão estratégias para verificar a legitimidade das mensagens e evitar possíveis fraudes.



d) Verificar a legitimidade de um sítio de compras online antes de efetuar uma compra: Os participantes irão representar o processo de verificação da legitimidade de um sítio de compras online antes de efetuarem uma compra. Examinarão as características de segurança do sítio, como a encriptação SSL e as opções de pagamento seguro, e discutirão estratégias para identificar retalhistas online de confiança.

Encoraje os participantes a refletirem em conjunto e a planearem a sua abordagem ao cenário da dramatização. Devem discutir as medidas que irão tomar para proteger eficazmente as suas contas e transações online.

Jogo de papéis (20 minutos):

Os participantes representam os cenários que lhes foram atribuídos, assumindo os papéis das pessoas envolvidas (por exemplo, titulares de contas, representantes do serviço de apoio ao cliente, hackers).

Incentive os participantes a envolverem-se em diálogos e ações realistas à medida que navegam no cenário e implementam medidas de segurança para impedir o acesso não autorizado.

Os facilitadores podem fornecer orientação e apoio conforme necessário, respondendo a perguntas e oferecendo sugestões para ajudar os participantes a navegar eficazmente pelos cenários.

Análise e debate (15 minutos):

Após a atividade de dramatização, reúna-se novamente com todo o grupo para um balanço e debate.

Convide os participantes a partilharem as suas experiências durante o exercício de dramatização, incluindo quaisquer desafios que tenham encontrado e a forma como os resolveram.

Facilite um debate sobre as principais conclusões e lições aprendidas com a atividade, realçando a importância de proteger as contas e transações online para evitar o acesso não autorizado.

Incentive os participantes a refletir sobre as suas próprias práticas de segurança online e a identificar áreas a melhorar com base nos cenários de dramatização.

Conclusão (5 minutos):

Resumir os principais pontos discutidos durante a atividade e reforçar a importância de medidas proactivas de segurança online.

Agradecer aos participantes a sua participação e empenhamento no exercício de dramatização.

Medidas básicas de segurança

As medidas básicas de segurança constituem a base de uma defesa sólida contra ameaças digitais. Utilizar palavras-passe fortes e únicas, ativar a autenticação de dois fatores (2FA) e atualizar regularmente o software e os dispositivos são passos essenciais para proteger as suas contas online e informações pessoais. Nas secções seguintes, iremos aprofundar cada um destes métodos, explorando a sua importância e fornecendo sugestões práticas de implementação.

Importância da utilização de palavras-passe fortes e únicas e métodos para as criar

Na era digital atual, as palavras-passe desempenham um papel crucial na segurança das nossas contas online e informações sensíveis. No entanto, a prevalência de ameaças cibernéticas, como ataques de phishing, violações de dados e ataques de força bruta, realça a importância de utilizar palavras-passe únicas e fortes para proteger as nossas contas contra o acesso não autorizado. Aqui estão várias razões pelas quais a utilização de palavras-passe únicas e fortes é essencial:

Prevenir o acesso não autorizado: As palavras-passe únicas e fortes funcionam como a primeira linha de defesa contra o acesso não autorizado às nossas contas online. Tornam

significativamente mais difícil para os cibercriminosos adivinharem ou decifrarem as palavras-passe através de ferramentas automatizadas ou ataques de força bruta.

Proteção de informações pessoais: As contas online contêm frequentemente informações pessoais e financeiras sensíveis, tais como dados bancários, registos médicos e comunicações pessoais. A utilização de palavras-passe fortes e únicas ajuda a proteger estas informações contra o acesso não autorizado, reduzindo o risco de roubo de identidade, fraude financeira e violações de privacidade.

Mitigar o impacto das violações de dados: Na eventualidade de uma violação de dados em que as credenciais de início de sessão sejam comprometidas, a existência de palavras-passe fortes e únicas para cada conta pode atenuar o impacto, impedindo que os cibercriminosos acedam a outras contas utilizando as mesmas credenciais. Esta prática, conhecida como higiene das palavras-passe, ajuda a conter os danos e a limitar a exposição a outros riscos de segurança.

Conformidade com as melhores práticas de segurança: As palavras-passe únicas e fortes estão em conformidade com as melhores práticas da indústria e as diretrizes de cibersegurança recomendadas por organizações como o National Institute of Standards and Technology (NIST) e a Cybersecurity and Infrastructure Security Agency (CISA). Seguir estas recomendações demonstra um compromisso com a segurança online e ajuda os indivíduos e as organizações a manterem-se em conformidade com os regulamentos e normas relevantes.

Métodos para criar palavras-passe fortes e únicas:

A criação de palavras-passe únicas fortes implica a utilização de uma combinação de caracteres, incluindo letras maiúsculas e minúsculas, números e símbolos especiais, para tornar as palavras-passe mais resistentes a tentativas de pirataria informática. Aqui estão alguns métodos para criar palavras-passe únicas e fortes:

Frases-senha: Em vez das palavras-passe tradicionais, considere a utilização de frases-passe - combinações mais longas de palavras ou frases que são fáceis de memorizar, mas

difíceis de adivinhar. As frases-chave podem ser compostas por palavras aleatórias, letras de canções, títulos de livros ou frases memoráveis com significado pessoal.

Combinações aleatórias de caracteres: Utilize uma combinação aleatória de letras maiúsculas e minúsculas, números e símbolos especiais para criar uma palavra-passe única. Evite utilizar padrões ou sequências facilmente adivinháveis, tais como "123456" ou "password", que são normalmente visados pelos hackers.

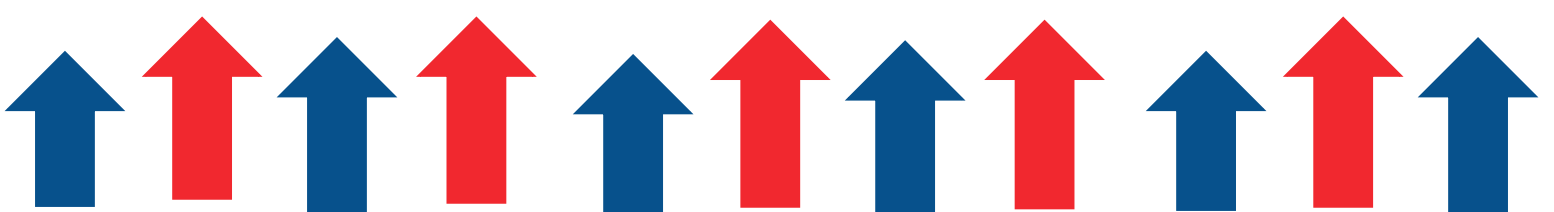
Geradores de palavras-passe: Considere a utilização de ferramentas geradoras de palavras-passe ou de funcionalidades incorporadas no software de gestão de palavras-passe para criar palavras-passe fortes e únicas. Os geradores de palavras-passe podem gerar palavras-passe aleatórias de vários comprimentos e complexidade, tornando-as altamente seguras e difíceis de adivinhar.

Evitar palavras de dicionário: Evite utilizar palavras de dicionário ou frases fáceis de adivinhar como palavras-passe, uma vez que estas são suscetíveis a ataques de dicionário e a ferramentas de quebra de palavras-passe. Em vez disso, opte por combinações de caracteres aleatórios ou frases-passe que não se encontrem em dicionários ou padrões de linguagem comuns.

Senhas exclusivas para cada conta: Certifique-se de que cada conta online tem uma palavra-passe única para evitar o efeito dominó de uma única palavra-passe comprometida que conduza ao acesso não autorizado a várias contas. Evite utilizar a mesma palavra-passe em várias contas, uma vez que tal aumenta o risco de violações e comprometimentos da segurança.

Visão geral da autenticação de dois fatores e o seu papel no reforço da segurança da conta

A autenticação de dois fatores (2FA) é uma camada adicional de segurança utilizada para proteger as contas online para além de um simples nome de utilizador e palavra-passe. Exige que os utilizadores forneçam dois fatores de autenticação diferentes para verificar a sua identidade e obter acesso às suas contas. Estes fatores de autenticação dividem-se normalmente em três categorias: algo que se sabe (por exemplo, uma palavra-passe), algo que se tem (por exemplo, um dispositivo móvel ou um token de hardware) e algo que se é (por exemplo, dados biométricos como impressões digitais ou reconhecimento facial).



Importância da autenticação de dois fatores:

Segurança reforçada: A 2FA melhora significativamente a segurança da conta, adicionando uma camada extra de proteção para além de uma simples palavra-passe. Mesmo que um hacker consiga obter a palavra-passe de um utilizador, continuará a precisar de aceder ao segundo fator (por exemplo, um dispositivo móvel ou dados biométricos) para se autenticar com êxito e obter acesso à conta.

Proteção contra o roubo de palavras-passe: O roubo de senhas é um método comum usado por hackers para obter acesso não autorizado a contas on-line. Ao exigir uma segunda forma de autenticação, a 2FA atenua o risco de acesso não autorizado, mesmo que as palavras-passe sejam comprometidas.

Redução do risco de acesso não autorizado: A 2FA reduz o risco de acesso não autorizado às contas, especialmente no caso de reutilização de palavras-passe ou de palavras-passe fracas. Mesmo que a palavra-passe de um utilizador seja comprometida devido a uma violação de dados ou a um ataque de phishing, o fator de autenticação adicional acrescenta uma camada extra de segurança.

Conformidade com as normas de segurança: Muitas organizações e órgãos reguladores recomendam ou exigem o uso da 2FA como parte de seus protocolos de segurança. A conformidade com estas normas ajuda a garantir que os dados e recursos sensíveis estão adequadamente protegidos contra o acesso não autorizado.

Sensibilização e controlo do utilizador: a 2FA aumenta a sensibilização e o controlo do utilizador relativamente à segurança da conta, fornecendo uma camada adicional de defesa contra o acesso não autorizado. Os utilizadores ficam habilitados a tomar medidas proactivas para proteger as suas contas e dados.

Métodos de autenticação de dois fatores:

Códigos de mensagem de texto (SMS): É enviado um código de verificação para o dispositivo móvel do utilizador através de uma mensagem de texto, que este deve introduzir juntamente com a sua palavra-passe para se autenticar.

Aplicações de autenticação: Os utilizadores podem instalar aplicações de autenticação como o Google Authenticator, o Microsoft Authenticator ou o Authy nos seus dispositivos móveis. Estas aplicações geram palavras-passe únicas baseadas no tempo (TOTPs) que os utilizadores introduzem juntamente com a sua palavra-passe para se autenticarem.

Tokens de hardware: Algumas organizações emitem tokens de hardware que geram códigos de autenticação. Os utilizadores têm de ter o token físico na sua posse para se autenticarem.

Autenticação biométrica: Alguns sistemas suportam métodos de autenticação biométrica, como impressões digitais, reconhecimento facial ou reconhecimento de voz, como segundo fator.

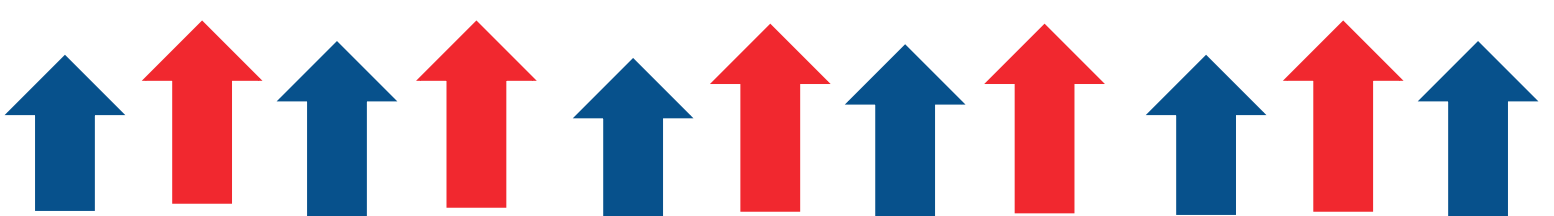
Importância da atualização regular do software e dos dispositivos para atenuar as vulnerabilidades de segurança

A importância da atualização regular do software e dos dispositivos para atenuar as vulnerabilidades de segurança não pode ser exagerada. Eis algumas das principais razões pelas quais é crucial:

Corrigir vulnerabilidades de segurança: As atualizações de software incluem frequentemente correcções que corrigem vulnerabilidades de segurança conhecidas. Essas vulnerabilidades podem ser exploradas por cibercriminosos para obter acesso não autorizado a sistemas, roubar informações confidenciais ou interromper serviços. As atualizações regulares ajudam a garantir que estas vulnerabilidades são resolvidas prontamente, reduzindo o risco de exploração.

Proteger-se contra exploits: Os cibercriminosos estão constantemente a desenvolver novas técnicas e explorações para atacar software e dispositivos. Ao manter o software e os dispositivos atualizados, os utilizadores podem proteger-se contra vulnerabilidades e explorações recentemente descobertas. Isto ajuda a manter a integridade e a segurança dos sistemas e dos dados.

Manter a conformidade: Em muitos sectores, a conformidade com regulamentos e normas relacionados com a cibersegurança é obrigatória. A atualização regular do software e dos dispositivos é frequentemente um requisito destes regulamentos e normas. O não



cumprimento destes requisitos pode resultar em penalizações, coimas ou outras consequências legais.

Melhorar a estabilidade e o desempenho: As atualizações de software não só resolvem as vulnerabilidades de segurança, como também incluem melhorias na estabilidade e no desempenho. Ao manter o software e os dispositivos atualizados, os utilizadores podem beneficiar de uma maior fiabilidade, de um desempenho mais rápido e de uma funcionalidade melhorada.

Proteja-se contra malware e ciberataques: O software e os dispositivos desatualizados são mais vulneráveis a infeções de malware e ciberataques. Os cibercriminosos exploram frequentemente vulnerabilidades conhecidas em software desatualizado para distribuir malware, como ransomware, vírus ou spyware. As atualizações regulares ajudam a proteger contra estas ameaças, colmatando as lacunas de segurança.

Manter o suporte do fornecedor: Normalmente, os fornecedores de software fornecem suporte e manutenção para os seus produtos durante um período limitado. Quando o software chega ao fim do seu ciclo de vida de suporte, os fornecedores podem deixar de lançar atualizações e patches, deixando os utilizadores vulneráveis a ameaças à segurança. A atualização regular do software e dos dispositivos garante que os utilizadores continuam a receber suporte do fornecedor e proteção contra vulnerabilidades de segurança.

Atividade: Workshop prático sobre a criação de palavras-passe fortes e a ativação da autenticação de dois fatores em várias plataformas online.

O objetivo deste workshop é informar os participantes sobre a importância de criar palavras-passe fortes e de ativar a autenticação de dois fatores (2FA) para aumentar a segurança das suas contas online. Os participantes aprenderão a criar e gerir palavras-passe fortes e a configurar a 2FA em diferentes plataformas online.

Materiais necessários:

Computadores ou dispositivos móveis com acesso à Internet para cada participante

Slides de apresentação ou folhetos sobre como criar palavras-passe fortes e ativar a 2FA

Exemplos de plataformas online que suportam a 2FA (por exemplo, Google, Facebook, Twitter, sítios Web de bancos)

Materiais de escrita

Instruções:

Introdução (10 minutos):

Dê as boas-vindas aos participantes no seminário e apresente a importância de criar palavras-passe fortes e de ativar a autenticação de dois fatores (2FA) para aumentar a segurança online.

Apresentar uma panorâmica da ordem de trabalhos do seminário e dos objetivos de aprendizagem.

Apresentação sobre a criação de palavras-passe fortes (15 minutos):

Apresentar uma breve panorâmica das características das palavras-passe fortes, incluindo o comprimento, a complexidade e a exclusividade.

Fornecer dicas e orientações para a criação de palavras-passe fortes, tais como a utilização de uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.

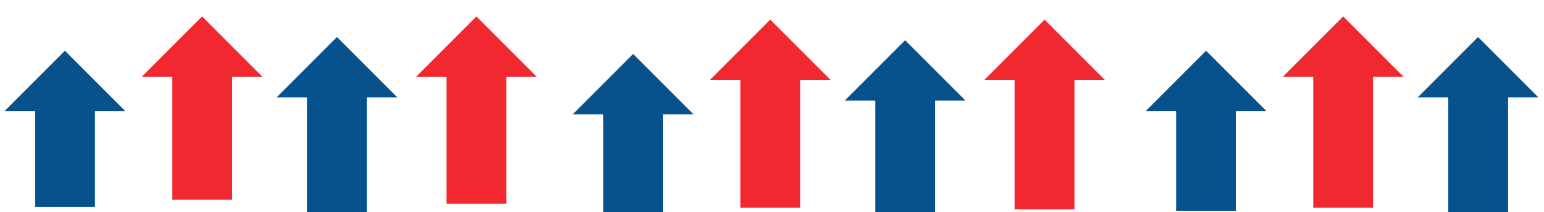
Demonstrar técnicas de gestão de palavras-passe, como a utilização de gestores de palavras-passe para gerar e armazenar palavras-passe fortes de forma segura.

Por exemplo:

1Password: Conhecido pela sua segurança imbatível e toneladas de funcionalidades extra. É uma escolha de topo para a maioria dos utilizadores e é particularmente adequada para famílias.

Dashlane: Oferece extras de destaque, como monitorização da dark web e uma VPN2 rápida. Também é conhecido pela sua gestão de palavras-passe de qualidade superior.

RoboForm: Um gestor de palavras-passe acessível com boa segurança e capacidades poderosas de preenchimento de formulários.



Keeper: Gestor de palavras-passe altamente seguro com aplicações intuitivas e preços flexíveis.

NordPass: Conhecido pela sua gestão segura de palavras-passe, é particularmente adequado para administradores de contas empresariais.

Bitwarden: Conhecido pela sua gestão gratuita de palavras-passe.

Estes gestores de palavras-passe podem ajudá-lo a criar palavras-passe únicas e fortes para cada uma das suas contas online e alertá-lo para potenciais fugas de dados. Todos eles são totalmente gratuitos ou muito económicos. Tenha em atenção que, embora estes gestores de palavras-passe forneçam serviços semelhantes, as funcionalidades exatas e os preços podem variar. É sempre uma boa ideia consultar os respetivos sítios Web oficiais para obter as informações mais precisas e atualizadas.

Atividade prática: Criar palavras-passe fortes (20 minutos):

Dividir os participantes em pares ou pequenos grupos.

Forneça aos participantes uma lista de contas online comuns (por exemplo, correio eletrónico, redes sociais, serviços bancários) e peça-lhes que criem palavras-passe fortes para cada conta.

Incentive os participantes a aplicar as diretrizes de criação de palavras-passe discutidas anteriormente e a garantir que cada palavra-passe é única e não é fácil de adivinhar.

Circular entre os grupos para ajudar e orientar conforme necessário.

Apresentação sobre a ativação da autenticação de dois fatores (2FA) (15 minutos):

Apresentar uma panorâmica da autenticação de dois fatores (2FA) e do seu papel no reforço da segurança das contas online.

Explicar os diferentes tipos de métodos 2FA, como códigos SMS, aplicações de autenticação e tokens de hardware.

Fornecer instruções passo a passo para ativar a 2FA em várias plataformas online, incluindo exemplos de plataformas que suportam a 2FA

Atividade prática: Ativação da autenticação de dois fatores (2FA) (20 minutos):

Instrua os participantes a escolherem uma plataforma online que suporte a 2FA (por exemplo, Google, Facebook, Twitter, sítio Web de um banco).

Orientar os participantes no processo de ativação da 2FA na plataforma escolhida, utilizando as instruções passo a passo fornecidas.

Incentive os participantes a utilizarem os seus dispositivos móveis ou computadores para acompanharem o processo e ativarem a 2FA nas suas contas.

Ajuda e apoio na resolução de problemas, conforme necessário.

Conclusão e debate (10 minutos):

Reúna os participantes para um breve resumo e debate.

Reveja as principais conclusões do workshop, incluindo a importância de criar palavras-passe fortes e de ativar a autenticação de dois fatores (2FA) para melhorar a segurança online.

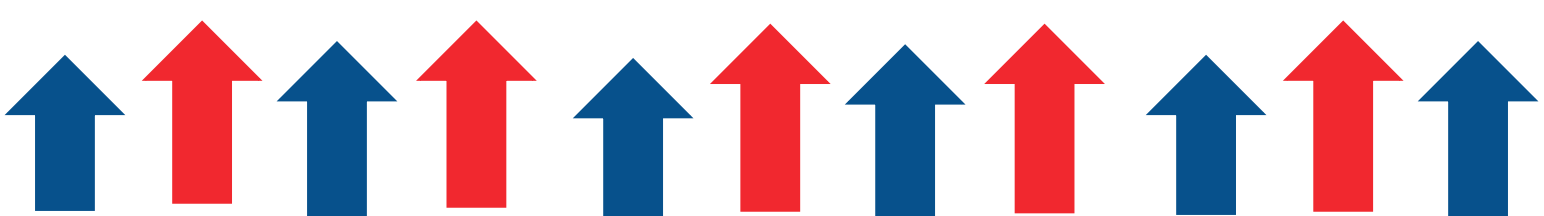
Incentive os participantes a partilharem as suas experiências e quaisquer desafios que tenham encontrado durante as atividades práticas.

Fornecer recursos adicionais e apoio aos participantes que pretendam saber mais sobre as melhores práticas de segurança online.

Conclusão:

Agradecer aos participantes pela sua participação e empenhamento no seminário.

Recorde aos participantes que devem aplicar os conhecimentos e competências que aprenderam para proteger as suas contas online e as suas informações pessoais.



Incentive os participantes a partilharem os seus novos conhecimentos com amigos, familiares e colegas para promoverem melhores práticas de segurança online.

Reconhecer as burlas

Abaixo são explorados os tipos mais comuns de burlas, as suas características e os sinais de alerta a que deve estar atento.

Os e-mails de phishing são e-mails fraudulentos que parecem ser de organizações ou indivíduos legítimos, mas que são concebidos para enganar os destinatários e levá-los a revelar informações sensíveis, tais como palavras-passe, nomes de utilizador, números de cartões de crédito ou outras informações pessoais. Estas mensagens de correio eletrónico contêm frequentemente ligações para sítios Web falsos ou anexos maliciosos.

Exemplo: Em 2016, um esquema de phishing generalizado visou os utilizadores do Gmail, enviando e-mails que pareciam ser da Google, levando os utilizadores a clicar numa ligação para uma página de início de sessão falsa da Google. Os utilizadores que introduziam as suas credenciais na página falsa forneciam inadvertidamente as suas informações de início de sessão aos atacantes, que obtinham então acesso não autorizado às suas contas.

Os esquemas Ponzi são esquemas de investimento fraudulentos que prometem rendimentos elevados aos investidores com pouco ou nenhum risco. Num esquema Ponzi, os primeiros investidores recebem rendimentos provenientes dos investimentos de investidores posteriores e não de lucros legítimos. À medida que o esquema cresce, o operador pode utilizar fundos de novos investidores para pagar rendimentos a investidores anteriores, criando a ilusão de rendibilidade.

Exemplo: Um dos esquemas Ponzi mais infames da história foi orquestrado por Bernie Madoff, que defraudou investidores em milhares de milhões de dólares ao longo de várias décadas. Madoff prometeu rendimentos consistentes e elevados aos investidores através da sua empresa de investimento, mas, em vez disso, estava a utilizar os fundos dos novos investidores para pagar rendimentos aos investidores existentes. O esquema acabou por entrar em colapso em 2008, levando a enormes perdas financeiras para milhares de investidores.

As burlas de investimento envolvem esquemas fraudulentos ou ofertas que prometem elevados rendimentos dos investimentos, mas que acabam por resultar em perdas financeiras para os investidores. Estas burlas visam frequentemente pessoas que procuram investir o seu dinheiro em oportunidades que parecem demasiado boas para serem verdadeiras.

Exemplo: Nos últimos anos, as fraudes de investimento em criptomoedas têm-se tornado cada vez mais frequentes. Os burlões podem promover ofertas iniciais de moedas (ICO) falsas ou oportunidades de investimento em criptomoedas falsas, prometendo retornos elevados com um risco mínimo. Estas burlas são concebidas para enganar os investidores e levá-los a enviar o seu dinheiro para os burlões, resultando em perdas financeiras para as vítimas.

Características de cada tipo de fraude e sinais de alerta a que deve estar atento

1. E-mails de phishing:

Características:

Os e-mails de phishing parecem muitas vezes ser de organizações legítimas, como bancos, plataformas de redes sociais ou agências governamentais.

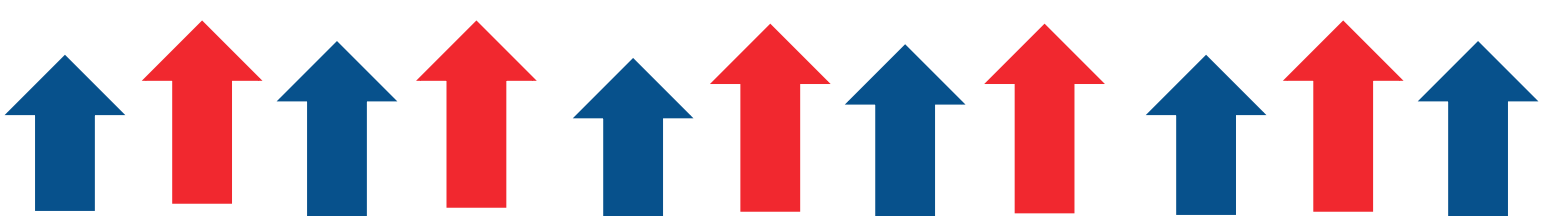
Normalmente, contêm mensagens urgentes ou alarmantes que incitam os destinatários a tomar medidas imediatas, como clicar numa ligação ou fornecer informações sensíveis.

Os e-mails de phishing podem incluir logótipos, marcas ou endereços de e-mail falsos que imitam fontes legítimas para enganar os destinatários.

Sinais de alerta a que estar atento:

Saudações genéricas: Os e-mails de phishing utilizam frequentemente saudações genéricas como "Caro cliente" em vez de se dirigirem aos destinatários pelo seu nome.

Pedidos urgentes: Os e-mails de phishing podem conter pedidos urgentes de informações pessoais, verificação de conta ou ação imediata para evitar consequências.



Hiperligações suspeitas: Desconfie de ligações em mensagens de correio eletrónico que o direccionem para sítios Web desconhecidos ou URLs que não correspondam ao domínio do remetente.

Gramática e ortografia incorrectas: Os e-mails de phishing contêm frequentemente erros ortográficos e gramaticais, formatação invulgar ou linguagem estranha que podem indicar que não provêm de uma fonte legítima.

Pedidos de informações pessoais: Normalmente, as organizações legítimas não solicitam informações sensíveis, como palavras-passe, números da Segurança Social ou detalhes de contas, por correio eletrónico.

2. Esquemas Ponzi:

Características:

Os esquemas Ponzi prometem rendimentos elevados sobre os investimentos com um risco mínimo.

Dependem de um afluxo contínuo de novos investidores para pagar rendimentos aos investidores existentes, em vez de gerarem lucros legítimos com os investimentos.

Os esquemas Ponzi utilizam frequentemente estratégias de investimento complexas ou jargão financeiro para confundir os investidores e criar a ilusão de legitimidade.

Sinais de alerta a que estar atento:

Rendimentos irrealistas: Tenha cuidado com as oportunidades de investimento que prometem rendimentos consistentemente elevados com pouco ou nenhum risco.

Falta de transparência: Os esquemas Ponzi carecem frequentemente de transparência relativamente à forma como os fundos dos investidores estão a ser utilizados ou investidos.

Pressão para investir: Os burlões podem utilizar táticas de venda de alta pressão para convencer as pessoas a investir rapidamente, sem dar tempo suficiente para a devida diligência ou investigação.

Sem registo ou regulamentação: As oportunidades de investimento legítimas estão normalmente registadas junto das autoridades reguladoras e sujeitas a supervisão. Os esquemas Ponzi podem não estar devidamente registados ou regulamentados.

3. Fraudes de investimento:

Características:

As burlas de investimento podem envolver ofertas ou oportunidades fraudulentas relacionadas com ações, bens imobiliários, criptomoedas ou outros produtos financeiros.

Os burlões podem utilizar informações falsas ou enganosas para induzir as pessoas a investir dinheiro.

As burlas de investimento prometem frequentemente rendimentos elevados com um mínimo de esforço ou risco, aproveitando-se do desejo das pessoas de obterem lucros rápidos.

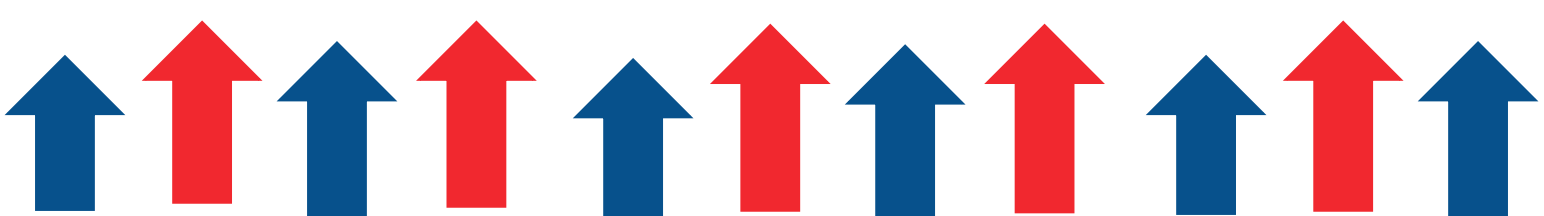
Sinais de alerta a que estar atento:

Ofertas não solicitadas: Tenha cuidado com as ofertas de investimento não solicitadas recebidas por correio eletrónico, chamadas telefónicas, redes sociais ou anúncios online.

Falta de documentação: As oportunidades de investimento legítimas fornecem normalmente documentação ou materiais de divulgação que descrevem os pormenores, riscos e termos do investimento. Desconfie de oportunidades que não tenham documentação ou transparência adequadas.

Pressão para agir rapidamente: Os burlões podem pressionar as pessoas a tomar decisões de investimento rapidamente, sem dar tempo suficiente para a devida diligência ou investigação.

Rendimentos garantidos: Seja cético em relação a oportunidades de investimento que garantam rendimentos elevados ou prometam um risco mínimo. Todos os investimentos implicam um certo grau de risco e as oportunidades de investimento legítimas não garantem lucros.



Atividade: Analisar as mensagens de correio eletrónico de phishing e identificar os elementos-chave que indicam que são fraudulentas

O objetivo desta atividade é informar os participantes sobre os principais elementos das mensagens de correio eletrónico de phishing e como identificá-las como fraudulentas. Os participantes analisarão mensagens de correio eletrónico de phishing reais e identificarão os sinais de alerta que indicam que se trata de uma fraude.

Materiais necessários:

Impressões ou cópias digitais de mensagens de correio eletrónico de phishing reais (certifique-se de que estas mensagens não contêm ligações ou anexos maliciosos)

Quadro branco ou flip chart

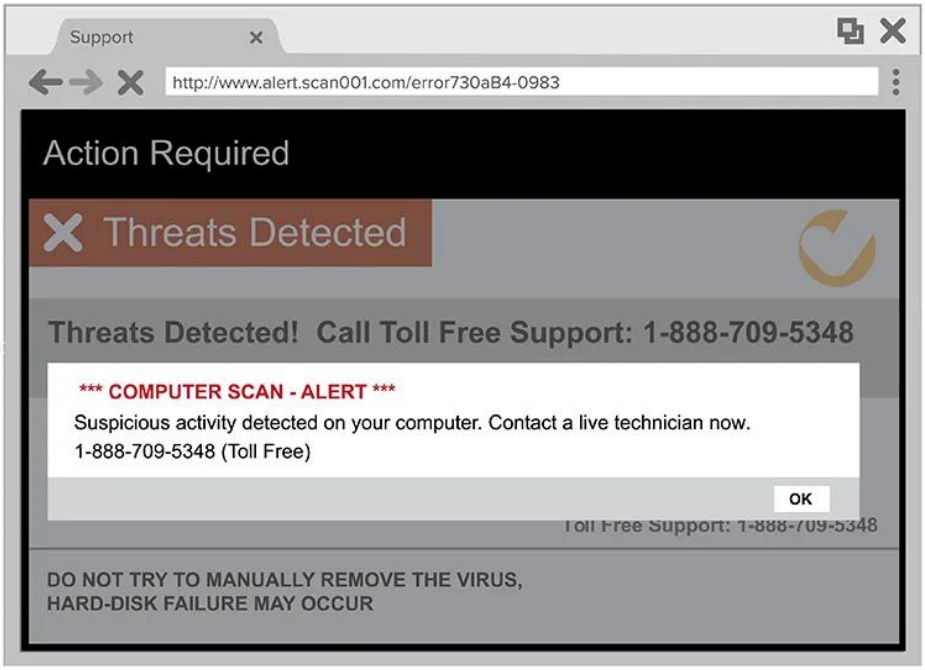
Materiais de escrita

Exemplos:

1. E-mails de phishing do suporte técnico

Utilizando táticas de medo em mensagens de correio eletrónico e pop-ups, os burlões enganam as vítimas, fazendo-as acreditar que precisam de apoio técnico. Os burlões podem fazer-se passar pela Microsoft - a marca mais falsificada em 2023 [*] - ou pelo Geek Squad da Best Buy para o convencer de que há um problema com o seu dispositivo.

Como funcionam os esquemas de apoio técnico:



Os burlões utilizam uma linguagem altamente técnica ou vaga em matéria de cibersegurança para o assustar, confundir e desarmar.

Podem faturar-lhe as reparações forçadas de dispositivos ou software - ou vender-lhe atualizações ou garantias desnecessárias.

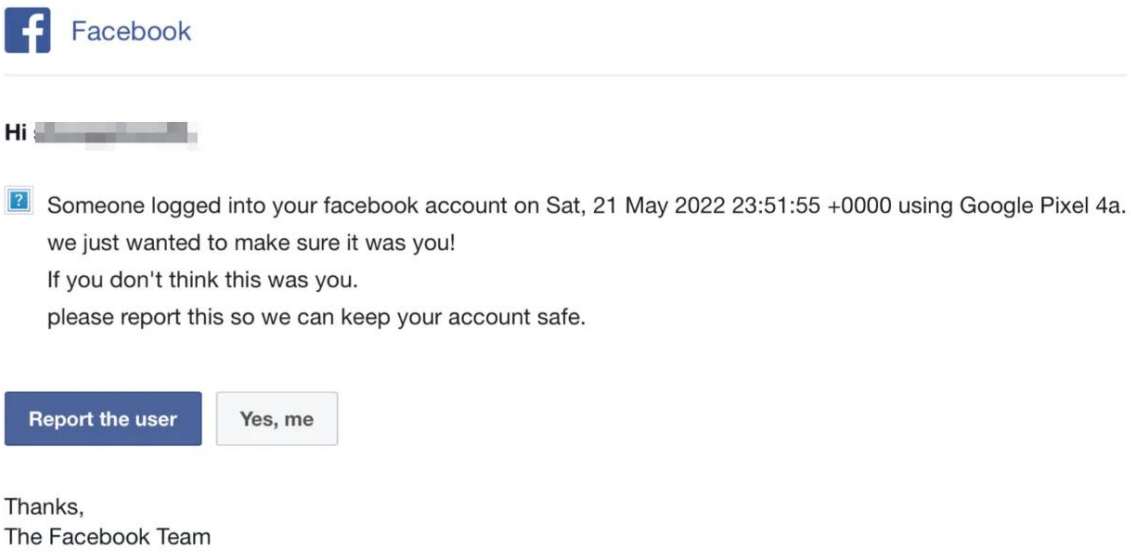
Podem incitá-lo a clicar em anexos maliciosos ou a visitar um sítio Web para obter as suas informações.

Podem pedir acesso remoto ao seu computador para resolver supostos problemas, permitindo-lhes instalar malware ou ransomware.

E-mails de phishing nas redes sociais

Neste esquema, o e-mail de phishing vem de uma alegada equipa de apoio de uma rede social, como o Instagram ou o LinkedIn. A mensagem imita um aviso típico ou uma notificação de conta para parecer autêntica e chamar a atenção do utilizador.

Falsa mensagem de correio eletrónico de alerta de início de sessão fazendo-se passar pelo Facebook, com um CTA para "Denunciar o utilizador".



Exemplo de um esquema de phishing nas redes sociais. Fonte: Reddit.

Como funcionam os esquemas de phishing nas redes sociais:

Este e-mail fraudulento contém uma ligação de phishing para verificar ou iniciar sessão na sua conta.

Clicar na ligação pode descarregar malware ou spyware ou levá-lo para uma página de início de sessão falsificada.

Uma vez na posse das informações da sua conta, os burlões podem iniciar sessão e bloqueá-lo ou utilizar o início de sessão noutro local se tiver reutilizado a sua palavra-passe.

Instruções:

Introdução (5 minutos):

Dê as boas-vindas aos participantes na atividade e explique o objetivo:

Analisar mensagens de correio eletrónico de phishing e identificar os elementos-chave que indicam que são fraudulentas.

Fornecer uma visão geral dos e-mails de phishing e da importância de saber reconhecê-los para se proteger contra ameaças cibernéticas.

Apresentação sobre os principais elementos dos e-mails de phishing (10 minutos):

Apresentar uma breve panorâmica dos principais elementos dos e-mails de phishing, incluindo características comuns e sinais de alerta.

Discuta elementos como saudações genéricas, pedidos urgentes, ligações ou anexos suspeitos, má gramática e ortografia e pedidos de informações pessoais.

Análise de e-mails de phishing (30 minutos):

Dividir os participantes em pequenos grupos.

Distribua cópias impressas ou digitais de mensagens eletrónicas de phishing reais para cada grupo analisar.

Instrua os participantes a examinarem cuidadosamente os e-mails de phishing e a identificarem os principais elementos que indicam que são fraudulentos.

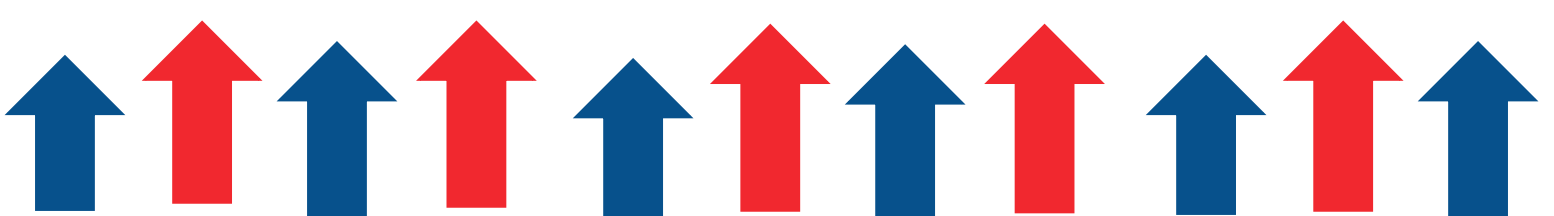
Incentive os participantes a debaterem as suas conclusões nos respetivos grupos e a anotarem os sinais de alerta que identificarem.

Discussão em grupo (15 minutos):

Voltem a reunir-se em grupo e convidem cada grupo a partilhar as suas observações e conclusões da análise das mensagens eletrónicas de phishing.

Facilitar um debate sobre os sinais de alerta comuns e os elementos-chave dos e-mails de phishing identificados pelos participantes.

Utilize um quadro branco ou um flipchart para registar os sinais de alerta e os elementos-chave identificados pelos participantes.



Reflexão e conclusões (10 minutos):

Conduza uma sessão de reflexão em que os participantes partilham as suas ideias e perceções obtidas através da análise de mensagens eletrónicas de phishing.

Discutir estratégias de proteção contra ataques de phishing, tais como verificar os endereços de correio eletrónico dos remetentes, evitar clicar em ligações ou anexos suspeitos e comunicar as tentativas de phishing às autoridades competentes.

Resumir as principais conclusões e sublinhar a importância da vigilância e do ceticismo quando se lida com mensagens de correio eletrónico não solicitadas.

Conclusão:

Agradeça aos participantes a sua participação na atividade e os seus contributos para o debate.

Incentivar os participantes a aplicar os conhecimentos e competências adquiridos para identificar e proteger-se contra e-mails de phishing na sua vida pessoal e profissional.

A importância da sensibilização para a cibersegurança

A sensibilização para a cibersegurança é fundamental para nos protegermos de várias ameaças online. Compreender as estratégias utilizadas pelos cibercriminosos para enganar os indivíduos, como as tentativas de phishing, é crucial para manter a segurança digital. Ao reconhecer as táticas de phishing comuns e ao distingui-las dos e-mails legítimos, as pessoas podem reduzir os riscos de serem vítimas de ciberataques.

Estratégias para reconhecer tentativas de phishing e distingui-las de e-mails legítimos

As tentativas de phishing têm frequentemente como objetivo enganar os destinatários para que divulguem informações sensíveis ou cliquem em ligações maliciosas. Ao empregar as seguintes estratégias, os indivíduos podem melhorar a sua capacidade de identificar e frustrar tentativas de phishing:

Verificar o endereço de correio eletrónico do remetente: Verifique cuidadosamente o endereço de correio eletrónico do remetente para garantir que corresponde ao domínio oficial da organização ou indivíduo que afirma ter enviado a mensagem de correio eletrónico. Desconfie de endereços de correio eletrónico que utilizem nomes de domínio mal escritos ou suspeitos.

Verifique se há saudações genéricas: Os e-mails de phishing utilizam frequentemente saudações genéricas como "Caro cliente" ou "Caro utilizador" em vez de se dirigirem aos destinatários pelo seu nome. As mensagens de correio eletrónico legítimas de organizações com boa reputação dirigem-se normalmente aos destinatários pelo seu nome.

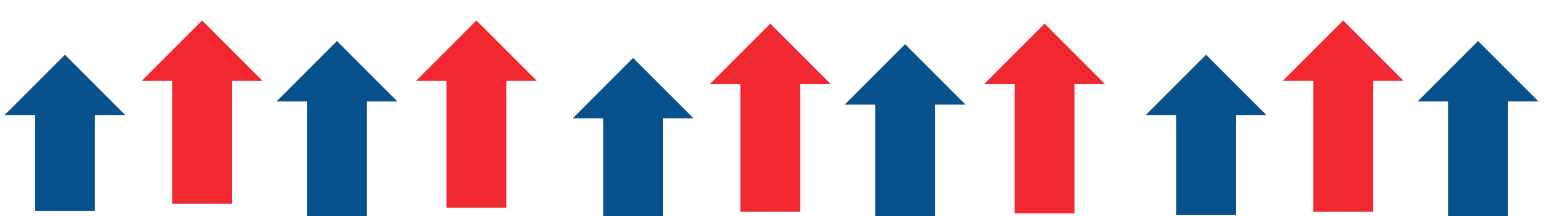
Procure pedidos urgentes ou ameaças: Os e-mails de phishing contêm frequentemente pedidos urgentes ou ameaças concebidas para criar uma sensação de urgência e pressionar os destinatários a tomarem medidas imediatas. Tenha cuidado com as mensagens de correio eletrónico que ameaçam consequências se não responder rapidamente ou não fornecer informações pessoais.

Examinar ligações e URLs: Passe o cursor do rato sobre as hiperligações nos e-mails (sem clicar) para pré-visualizar o URL de destino. Verifique se o URL corresponde ao sítio Web oficial da organização de que diz ser proveniente. Tenha cuidado com URLs encurtados ou URLs que redirecionam para sites desconhecidos ou suspeitos.

Evitar clicar em anexos: Tenha cuidado com os anexos de correio eletrónico, especialmente se vierem de fontes desconhecidas ou inesperadas. Os e-mails de phishing podem conter anexos maliciosos que podem instalar malware no seu dispositivo ou comprometer a sua segurança.

Verifique os pedidos de informações pessoais: Seja cético em relação a e-mails que solicitem informações confidenciais, como palavras-passe, números da Segurança Social, detalhes de cartões de crédito ou credenciais de contas. Normalmente, as organizações legítimas não solicitam informações confidenciais por correio eletrónico.

Verifique se existem erros ortográficos e gramaticais: Os e-mails de phishing contêm frequentemente erros ortográficos e gramaticais, uma estrutura de frases invulgar ou uma



linguagem estranha que pode indicar que não provêm de uma fonte legítima. Desconfie de mensagens de correio eletrónico com má qualidade de linguagem.

Seja cauteloso com pedidos ou ofertas invulgares: Desconfie de e-mails que ofereçam recompensas inesperadas, prémios ou negócios que pareçam demasiado bons para serem verdade. Os e-mails de phishing também podem pedir aos destinatários que participem em inquéritos, concursos ou ofertas que exijam informações pessoais ou transações financeiras.

Confie nos seus instintos e seja cético: Se algo parecer estranho ou suspeito numa mensagem de correio eletrónico, confie nos seus instintos e seja cauteloso. É melhor ser cético e verificar a legitimidade de uma mensagem de correio eletrónico antes de tomar qualquer medida.

Utilize software de segurança e filtros de correio eletrónico: Instale software antivírus e filtros de correio eletrónico de boa reputação para ajudar a detetar e bloquear tentativas de phishing. Estas ferramentas podem ajudar a identificar mensagens de correio eletrónico suspeitas e proteger contra conteúdos maliciosos.

Diretrizes para evitar clicar em ligações suspeitas ou descarregar anexos de fontes desconhecidas

Verificar a identidade do remetente: Antes de clicar em quaisquer ligações ou descarregar anexos, verifique a identidade do remetente. Certifique-se de que o correio eletrónico ou a mensagem provém de uma fonte legítima e não de um remetente desconhecido ou suspeito.

Verificar o endereço de correio eletrónico: Examine cuidadosamente o endereço de correio eletrónico do remetente. Tenha cuidado com os endereços de correio eletrónico que utilizam nomes de domínio com erros ortográficos ou suspeitos, uma vez que podem ser indicativos de tentativas de phishing.

Passe o rato sobre as hiperligações para pré-visualizar URLs: Passe o cursor do rato sobre hiperligações em e-mails ou mensagens (sem clicar) para pré-visualizar o URL de destino. Verifique se o URL corresponde ao sítio Web oficial da organização da qual afirma ser

proveniente. Tenha cuidado com URLs encurtados ou URLs que redirecionam para sites desconhecidos ou suspeitos.

Evitar mensagens ou e-mails não solicitados: Desconfie de e-mails ou mensagens não solicitados de remetentes desconhecidos, especialmente se contiverem hiperligações ou anexos. Elimine ou ignore essas mensagens de correio eletrónico para evitar potenciais riscos de segurança.

Cuidado com pedidos urgentes ou suspeitos: Tenha cuidado com e-mails ou mensagens que contenham pedidos urgentes ou ameaças, tais como avisos de suspensão de conta, ação legal ou consequências financeiras. Os burlões utilizam frequentemente a urgência para pressionar os destinatários a clicarem em ligações maliciosas ou a descarregarem anexos.

Verificar o conteúdo com o remetente: Se receber uma mensagem de correio eletrónico ou uma mensagem com ligações ou anexos de um remetente conhecido, mas o conteúdo parecer suspeito, verifique a legitimidade do conteúdo com o remetente através de um canal de comunicação separado (por exemplo, chamada telefónica ou mensagem de texto).

Utilizar software antivírus e filtros de correio eletrónico: Instale software antivírus e filtros de correio eletrónico de boa reputação nos seus dispositivos para ajudar a detetar e bloquear conteúdos maliciosos, incluindo ligações e anexos suspeitos. Mantenha o software antivírus e os filtros de correio eletrónico atualizados para uma eficácia máxima.

Informe-se sobre as táticas comuns de phishing: Mantenha-se informado sobre as táticas e estratégias de phishing comuns utilizadas pelos cibercriminosos para enganar as pessoas, levando-as a clicar em ligações maliciosas ou a descarregar anexos. Informe-se a si e aos membros da sua equipa sobre as últimas tendências e técnicas de phishing.

Seja cauteloso nas redes sociais e nas aplicações de mensagens: Tenha cuidado quando clicar em ligações ou descarregar anexos de plataformas de redes sociais, aplicações de mensagens ou outras plataformas online. Os burlões utilizam frequentemente estas plataformas para distribuir ligações de phishing e malware.

Comunicar atividades suspeitas: Se receber uma mensagem de correio eletrónico ou uma mensagem suspeita que contenha ligações ou anexos, comunique-a ao departamento de TI

da sua organização ou às autoridades competentes. A comunicação de atividades suspeitas pode ajudar a proteger outras pessoas de serem vítimas de esquemas de phishing.

Importância de manter a privacidade das informações pessoais nas plataformas de redes sociais

Manter a privacidade das informações pessoais nas plataformas de redes sociais é crucial por várias razões:

Proteção contra o roubo de identidade: As informações pessoais partilhadas nas redes sociais, como o nome completo, a data de nascimento, a morada e os dados de contacto, podem ser exploradas por ladrões de identidade para roubar a sua identidade. Com estas informações, os criminosos podem abrir contas fraudulentas, pedir cartões de crédito ou cometer outras formas de fraude financeira em seu nome.

Prevenção da ciberperseguição e do assédio: Partilhar demasiadas informações pessoais nas redes sociais pode torná-lo vulnerável à ciberperseguição e ao assédio. Indivíduos mal-intencionados podem utilizar as suas informações pessoais para seguir o seu paradeiro, monitorizar as suas atividades ou assediá-lo online ou na vida real.

Evitar as burlas online e os ataques de phishing: Os cibercriminosos utilizam frequentemente informações pessoais partilhadas nas redes sociais para lançar ataques de phishing ou burlas. Podem utilizar os seus dados pessoais para criar mensagens ou e-mails convincentes, induzindo-o a revelar informações sensíveis ou a cair em esquemas fraudulentos.

Proteção da reputação e da privacidade: A partilha de informações sensíveis ou inadequadas nas redes sociais pode prejudicar a sua reputação e privacidade. Os empregadores, colegas, familiares e outras pessoas podem ter acesso aos seus perfis nas redes sociais e os conteúdos inadequados podem ter consequências negativas na sua vida profissional e pessoal.

Prevenção de ataques de engenharia social: As plataformas de redes sociais são normalmente utilizadas por cibercriminosos para ataques de engenharia social, em que manipulam os utilizadores para que revelem informações confidenciais ou realizem ações

que comprometam a segurança. Ao limitar a quantidade de informações pessoais que partilha nas redes sociais, reduz o risco de ser vítima de táticas de engenharia social.

Segurança online melhorada: Manter as informações pessoais privadas nas plataformas de redes sociais ajuda a melhorar a sua segurança online geral. Reduz a probabilidade de acesso não autorizado às suas contas, minimiza o risco de roubo de identidade e fraude, e protege a sua privacidade e pegada digital.

Atividade: Sessão interativa sobre como identificar e evitar ligações e anexos suspeitos em cenários simulados de correio eletrónico.

O objetivo desta atividade é ensinar aos participantes como identificar e evitar ligações e anexos suspeitos em mensagens de correio eletrónico através de cenários simulados. Os participantes participarão em exercícios interativos para analisar o conteúdo das mensagens de correio eletrónico, identificar sinais de alerta e tomar decisões informadas sobre como clicar em ligações ou descarregar anexos.

Materiais necessários:

Cenários simulados de correio eletrónico

Quadro branco ou flip chart

Materiais de escrita

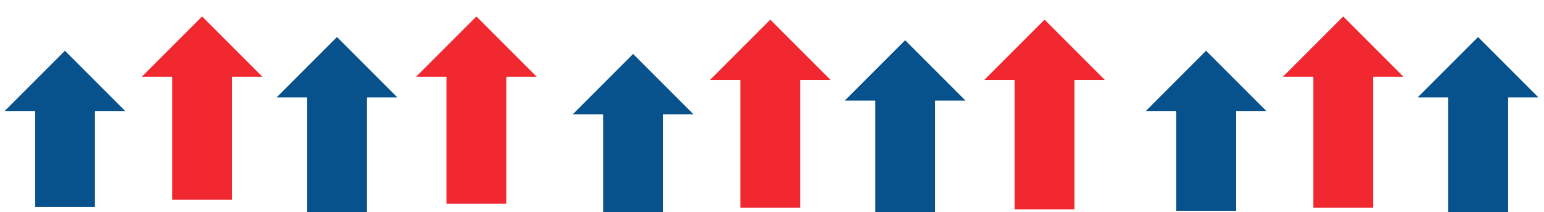
Computadores ou dispositivos móveis com acesso à Internet (opcional)

Instruções:

Introdução (5 minutos):

Dê as boas-vindas aos participantes na sessão interativa sobre como identificar e evitar ligações e anexos suspeitos em mensagens de correio eletrónico.

Explicar o objetivo da atividade: aumentar a sensibilização e as competências dos participantes para reconhecerem tentativas de phishing e se protegerem contra ciberameaças.



Apresentação sobre sinais de alerta e boas práticas (10 minutos):

Fazer uma breve apresentação sobre os sinais de alerta e as melhores práticas para identificar ligações e anexos suspeitos em mensagens de correio eletrónico.

Discutir as características comuns dos e-mails de phishing, tais como saudações genéricas, pedidos urgentes, URLs suspeitos e pedidos de informações pessoais.

Rever as melhores práticas para evitar clicar em ligações ou descarregar anexos de fontes desconhecidas ou suspeitas.

Cenários simulados de correio eletrónico (30 minutos):

Dividir os participantes em pequenos grupos.

Distribua cenários simulados de correio eletrónico a cada grupo. Cada cenário deve incluir uma mensagem de correio eletrónico com uma ligação ou um anexo que possa ser suspeito.

Por exemplo:

E-mail legítimo de um banco:

```
Assunto: O seu extrato mensal está pronto

De: noreply@yourbank.com

Caro cliente,

O seu extrato mensal está agora disponível na sua conta bancária online. Inicie sessão na sua conta para ver o extrato.

Cumprimentos,

O seu banco
```

E-mail de phishing que se faz passar por um banco:

```
Assunto: Urgente: Conta suspensa
```

De: support@yourbank-security.com

Caro cliente,

Detetámos uma atividade invulgar na sua conta. A sua conta foi suspensa. Clique na ligação abaixo para verificar a sua identidade e restaurar a sua conta.

Clique aqui para restaurar a sua conta.

Cumprimentos,

O seu banco

Neste caso, a mensagem de correio eletrónico utiliza uma linguagem urgente para assustar o destinatário e levá-lo a clicar na ligação. O endereço de correio eletrónico do remetente também é suspeito e não é o correio eletrónico oficial do banco.

E-mail legítimo de um colega:

Assunto: Notas de reunião

De: colleague@yourcompany.com

Olá,

Em anexo, encontram-se as notas da reunião.

Cumprimentos,

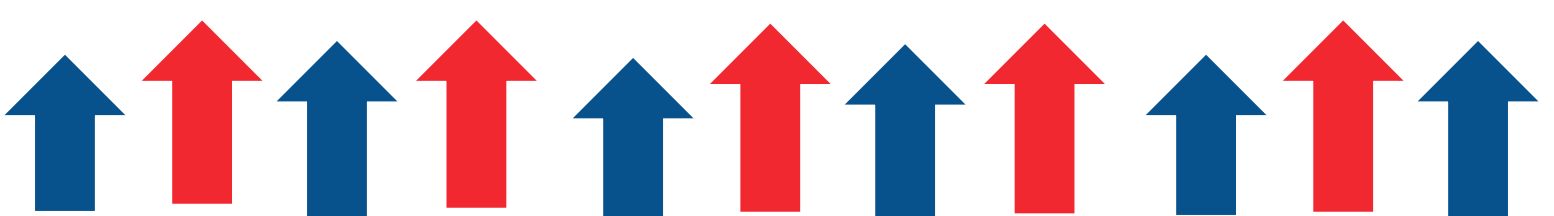
Colega

E-mail de phishing que se faz passar por um colega:

Assunto: Urgente: Fatura a vencer

De: colleage@yourcompany.com

Olá,



A fatura do nosso fornecedor está a vencer. Consulte a fatura em anexo e efetue o pagamento imediatamente.

Cumprimentos,

Colega

Neste caso, a mensagem de correio eletrónico utiliza uma linguagem urgente e pede ao destinatário que tome uma ação que normalmente não faz parte do seu trabalho. O endereço de correio eletrónico do remetente também contém um erro de digitação, o que pode ser um sinal de uma tentativa de phishing.

Instrua os participantes a analisar cuidadosamente o conteúdo da mensagem de correio eletrónico, a identificar sinais de alerta e a decidir se devem clicar na ligação ou descarregar o anexo.

Incentive os participantes a debaterem as suas observações e o processo de tomada de decisão nos seus grupos.

Discussão em grupo (15 minutos):

Voltem a reunir-se em grupo e convidem cada grupo a partilhar a sua análise dos cenários simulados de correio eletrónico.

Facilite um debate sobre os sinais de alerta identificados pelos participantes e a lógica subjacente às suas decisões de clicar em ligações ou descarregar anexos.

Utilize um quadro branco ou um flipchart para documentar as principais conclusões e ideias do debate.

Reflexão e conclusões (10 minutos):

Conduzir uma sessão de reflexão em que os participantes partilham as suas ideias e perceções obtidas na sessão interativa.

Discutir estratégias para evitar ser vítima de tentativas de phishing e proteger-se contra ciberameaças nas comunicações diárias por correio eletrónico.

Resumir as principais conclusões e sublinhar a importância da vigilância e do ceticismo quando se lida com ligações e anexos suspeitos em mensagens de correio eletrónico.

Conclusão:

Agradecer aos participantes pela sua participação ativa na sessão interativa.

Incentivar os participantes a aplicar os conhecimentos e competências adquiridos para identificar e evitar ligações e anexos suspeitos nas suas comunicações por correio eletrónico.

Fornecer recursos e apoio adicionais aos participantes que pretendam saber mais sobre as melhores práticas de cibersegurança.

Integração de estudos de caso

Exemplos reais de pessoas que foram vítimas de burlas financeiras.

O esquema Ponzi de Bernie Madoff:

Uma das mais notórias fraudes financeiras da história foi orquestrada por Bernie Madoff. Madoff geriu um esquema Ponzi durante várias décadas, prometendo rendimentos elevados aos investidores. Ele atraiu milhares de investidores, incluindo indivíduos, instituições de caridade e investidores institucionais, oferecendo retornos consistentes e lucrativos. No entanto, em vez de investir os fundos como prometido, Madoff utilizou o dinheiro dos novos investidores para pagar rendimentos aos investidores existentes. O esquema acabou por entrar em colapso em 2008, resultando em perdas de milhares de milhões de dólares para os investidores. (Hayes, 2023)

Fraude de adiantamento de taxas:

A fraude de adiantamento de honorários, também conhecida como **419 scams ou Nigerian prince scams**, é uma fraude financeira comum que visa indivíduos através de correio eletrónico ou outros canais de comunicação. Num esquema de fraude de adiantamento de honorários, os burlões prometem uma grande soma de dinheiro em troca de um pequeno pagamento adiantado ou honorário. As vítimas são atraídas com promessas de herança,

prémios de lotaria ou oportunidades de negócio, mas acabam por perder dinheiro para os burlões. (Grigutytė & Grigutytė, 2023)

Análise das estratégias que poderiam ter sido utilizadas para evitar ser vítima destas fraudes

O esquema Ponzi de Bernie Madoff:

Diligência devida: Os investidores poderiam ter efectuado uma diligência rigorosa antes de investir o seu dinheiro com Bernie Madoff. Isto implicaria verificar a legitimidade da empresa de investimento, examinar as demonstrações financeiras e procurar auditorias independentes de terceiros.

Questionar os retornos irrealistas: Os investidores deveriam ter questionado os rendimentos irrealistas e consistentes prometidos pela empresa de investimento de Madoff. Rendimentos consistentemente elevados com um risco mínimo deveriam ter levantado bandeiras vermelhas e levado a uma investigação mais aprofundada.

Golpes de phishing por e-mail:

Verificar a identidade do remetente: Verifique sempre a identidade do remetente antes de responder a mensagens de correio eletrónico que solicitem informações pessoais ou financeiras. As organizações legítimas não pedem informações sensíveis por correio eletrónico.

Examinar URLs e hiperligações: Passe o rato sobre hiperligações em mensagens de correio eletrónico para verificar o URL de destino antes de clicar. Tenha cuidado com os URLs que não correspondem ao sítio Web oficial da organização ou que contêm domínios suspeitos.

Fraudes de investimento em criptomoeda:

Pesquisar oportunidades de investimento: Efetuar uma pesquisa exaustiva antes de investir em criptomoedas ou participar em ofertas iniciais de moedas (ICO). Verifique a legitimidade do projeto, dos membros da equipa e dos documentos técnicos para evitar investir em esquemas fraudulentos.

Evitar rendimentos irrealistas: Seja cético em relação às oportunidades de investimento que prometem rendimentos consistentemente elevados com um risco mínimo. Os investimentos em criptomoeda, como qualquer outro investimento, têm riscos inerentes e os retornos garantidos devem ser vistos com desconfiança.

Fraude de adiantamento de taxas:

Seja cético em relação a ofertas não solicitadas: Desconfie de mensagens de correio eletrónico ou mensagens não solicitadas que prometam grandes somas de dinheiro em troca de um pequeno pagamento inicial ou de uma taxa. Tenha cuidado e questione a legitimidade de tais ofertas.

Pesquisar e verificar: Pesquise a oferta e verifique a identidade do remetente ou da organização antes de responder. As oportunidades de negócio legítimas não requerem normalmente pagamentos ou taxas iniciais.

Fraude de investimento:

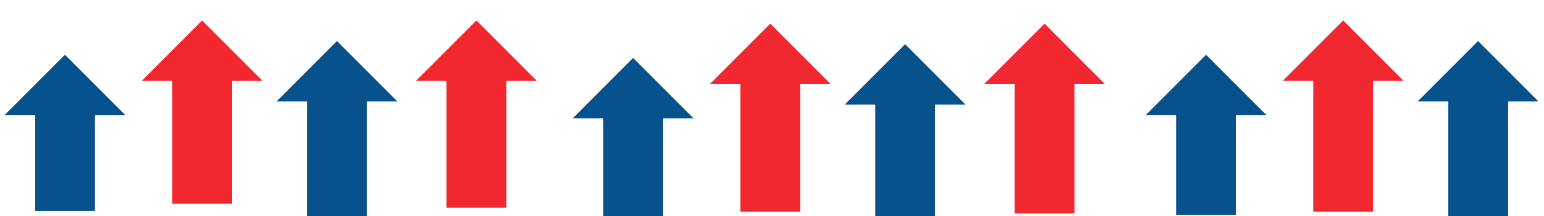
Verificar as oportunidades de investimento: Efetuar uma pesquisa exaustiva sobre as oportunidades de investimento e verificar a legitimidade da empresa de investimento ou do consultor. Verifique os registos regulamentares, as licenças e o historial disciplinar para garantir a credibilidade.

Evitar táticas de venda de alta pressão: Tenha cuidado com as oportunidades de investimento que utilizam táticas de venda de alta pressão ou que o apressam a tomar decisões rápidas. As oportunidades de investimento legítimas dão tempo para a devida diligência e consideração.

Atividade: Apresentação em grupo da análise de casos reais de burla financeira e proposta de medidas preventivas.

O objetivo desta atividade é aprofundar a compreensão dos participantes sobre casos reais de burla financeira, analisar os fatores que contribuíram para as burlas e propor medidas preventivas para se protegerem contra burlas semelhantes no futuro.

Materiais necessários:



- Lista de casos reais de burla financeira (mencionados acima)
- Materiais de apresentação (diapositivos, folhetos, etc.)
- Materiais de escrita
- Projetor ou ecrã (se utilizar diapositivos)

Instruções:

Introdução (10 minutos):

Dê as boas-vindas aos participantes na apresentação em grupo sobre a análise de casos reais de burla financeira e proponha medidas preventivas.

Explicar o objetivo da atividade: examinar casos reais de burla financeira, identificar padrões e vulnerabilidades comuns e propor medidas preventivas para reduzir o risco de burlas semelhantes.

Seleção de casos de burla (10 minutos):

Dividir os participantes em pequenos grupos.

Forneça a cada grupo uma lista de casos reais de burla financeira para escolher. Estes casos devem abranger uma variedade de burlas financeiras, como esquemas Ponzi, fraudes de investimento, burlas de phishing, etc.

Peça a cada grupo que selecione um caso de fraude para analisar e apresentar.

Investigação e análise (30 minutos):

Atribua tempo a cada grupo para pesquisar e analisar o caso de fraude selecionado.

Incentive os grupos a examinarem os pormenores do caso de burla, incluindo os autores, as vítimas, os métodos utilizados, os sinais de alerta, o impacto e as consequências.

Instrua os grupos a identificarem padrões comuns, vulnerabilidades e fatores que contribuíram para o sucesso da burla.

Medidas preventivas (30 minutos):

Depois de analisarem o caso da burla, dêem instruções a cada grupo para fazer um brainstorming e propor medidas preventivas para se protegerem contra burlas semelhantes no futuro.

Incentivar os grupos a considerar uma série de medidas preventivas, incluindo reformas regulamentares, educação dos consumidores, campanhas de sensibilização, soluções tecnológicas e ações de aplicação.

Cada grupo deve preparar uma lista de medidas preventivas e dar-lhes prioridade com base na sua eficácia e viabilidade.

Apresentações em grupo (40 minutos):

Atribuir tempo a cada grupo para apresentar a sua análise do caso de fraude e propor medidas preventivas.

Incentive os grupos a utilizar materiais de apresentação (diapositivos, folhetos, etc.) para apoiar as suas apresentações.

Após cada apresentação, facilite uma breve sessão de perguntas e respostas para que os outros participantes possam fazer perguntas e dar feedback.

Debate e reflexão (20 minutos):

Concluir as apresentações em grupo com uma sessão de debate e reflexão.

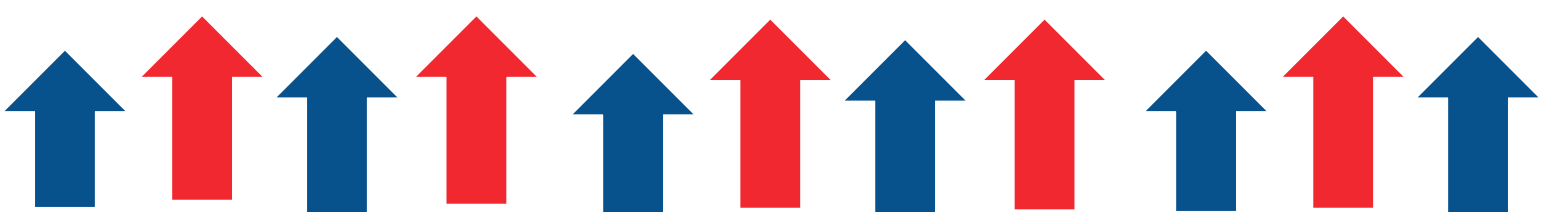
Incentivar os participantes a debater temas comuns, ideias e lições aprendidas com os casos de burla e as medidas preventivas propostas.

Facilitar o debate sobre a importância de medidas proactivas na prevenção de fraudes financeiras e na proteção dos consumidores e investidores.

Conclusão (10 minutos):

Agradecer aos participantes a sua participação e os seus contributos para as apresentações em grupo.

Resumir as principais conclusões e ideias da atividade.



Salientar a importância da vigilância permanente, da educação dos consumidores e dos esforços regulamentares no combate às fraudes financeiras.

Praticar

Atividade de aprendizagem autodirigida

Sugerir aos participantes que se informem mais sobre os tópicos e sugerir algumas leituras adicionais, como por exemplo:

Roubo de identidade, transações fraudulentas e ameaças à cibersegurança:

Identity Theft Resource Centre (https://www.idtheftcenter.org/) - Oferece informações, recursos e assistência às vítimas de roubo de identidade.

Sítio Web sobre roubo de identidade da Comissão Federal do Comércio (FTC) (https://www.identitytheft.gov/) - Fornece orientações passo a passo sobre prevenção, deteção e recuperação de roubo de identidade.

Importância das medidas de segurança e medidas básicas de segurança:

StaySafeOnline.org (https://staysafeonline.org/) - Fornece recursos e sugestões para a segurança online e sensibilização para a cibersegurança.

Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/) - Oferece recursos de cibersegurança, dicas e melhores práticas para indivíduos e organizações.

Reconhecer as burlas e a sensibilização para a cibersegurança:

FBI Internet Crime Complaint Centre (IC3) (https://www.ic3.gov/) - Permite aos utilizadores denunciar crimes na Internet e fornece recursos para a prevenção do cibercrime.

Better Business Bureau (BBB) Scam Alerts (https://www.bbb.org/scamtracker) - Oferece alertas de burla, dicas e recursos para consumidores e empresas.

Estudos de casos reais de burlas e estratégias para as evitar:

Securities and Exchange Commission (SEC) (https://www.sec.gov/) - Oferece recursos e informações sobre educação dos investidores, alertas e ações de execução.

Consumer Financial Protection Bureau (CFPB) (https://www.consumerfinance.gov/) - Disponibiliza recursos e ferramentas para os consumidores, incluindo alertas de fraude e relatórios sobre burlas financeiras.

Avaliação do questionário

Questionário: Identificar os riscos de segurança comuns e reconhecer as características das burlas

Instruções:

Lê cada pergunta com atenção e seleciona a melhor resposta.

Escolha a opção que melhor representa a resposta correta.

No final do teste, faça o balanço da sua pontuação para ver o seu desempenho.

O que é a usurpação de identidade?

Um tipo de malware que infecta computadores e rouba informações pessoais.

A utilização não autorizada das informações pessoais de outra pessoa para cometer fraudes ou outros crimes.

Uma fraude financeira que envolve esquemas de investimento fraudulentos.

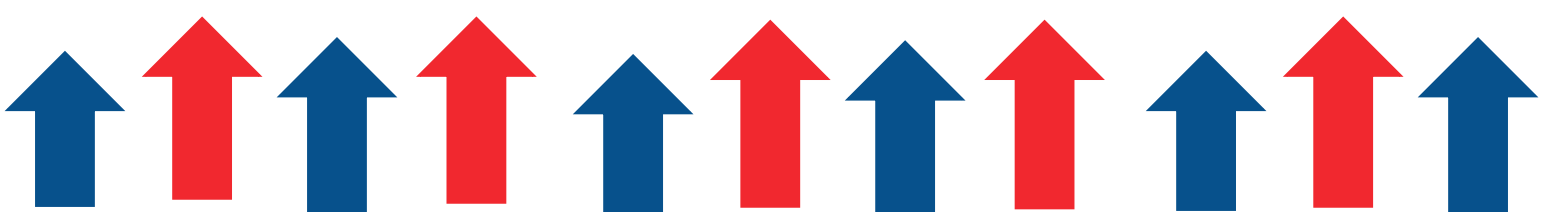
Uma ameaça de cibersegurança que visa contas bancárias online.

Qual das seguintes é uma caraterística dos e-mails de phishing?

Saudações personalizadas dirigidas ao destinatário pelo nome.

Pedidos de informações sensíveis, como palavras-passe ou números de cartões de crédito.

Endereços de correio eletrónico de remetentes legítimos que correspondem ao domínio oficial da organização.



Logótipos e marcas oficiais de organizações de confiança.

O que é um esquema Ponzi?

Um tipo de ataque de phishing que visa indivíduos através de mensagens de correio eletrónico fraudulentas.

Um esquema de investimento que promete rendimentos elevados aos investidores com um risco mínimo.

Uma ameaça à cibersegurança que explora vulnerabilidades em software ou sistemas.

Um tipo de malware concebido para roubar informações pessoais dos computadores.

Qual é o objetivo da autenticação de dois fatores?

Proteger as contas online, exigindo múltiplas formas de verificação.

Para evitar ataques de phishing através da encriptação das comunicações por correio eletrónico.

Para se proteger contra a usurpação de identidade, monitorizando os relatórios de crédito.

Para detetar e remover malware de dispositivos infetados.

Qual das seguintes opções é um sinal de alerta de uma potencial burla?

Pedidos urgentes de informações pessoais ou de ação imediata.

E-mails personalizados dirigidos ao destinatário pelo nome.

Logótipos e marcas oficiais de organizações conceituadas.

Pedidos de feedback ou inquéritos de fontes fidedignas.

Qual é a importância das atualizações regulares do software e da manutenção dos dispositivos?

Para proteção contra ataques de phishing e infeções por malware.

Proteger as contas online com palavras-passe fortes.

Para evitar a usurpação de identidade e a fraude financeira.

Atenuar as vulnerabilidades de segurança e proteger contra as ciberameaças.

Qual das seguintes opções NÃO é uma caraterística comum das oportunidades de investimento legítimas?

Rendimentos elevados garantidos com um risco mínimo.

Registo e supervisão regulamentares adequados.

Documentação transparente que descreve os pormenores e os riscos do investimento.

Pressão para tomar decisões de investimento rápidas sem a devida diligência.

Qual é a importância de manter as informações pessoais privadas nas plataformas das redes sociais?

Para proteção contra a usurpação de identidade e a perseguição cibernética.

Para evitar ataques de phishing e infeções por malware.

Para proteger contas online com autenticação de dois fatores.

Para evitar vulnerabilidades de software e problemas de manutenção do dispositivo.

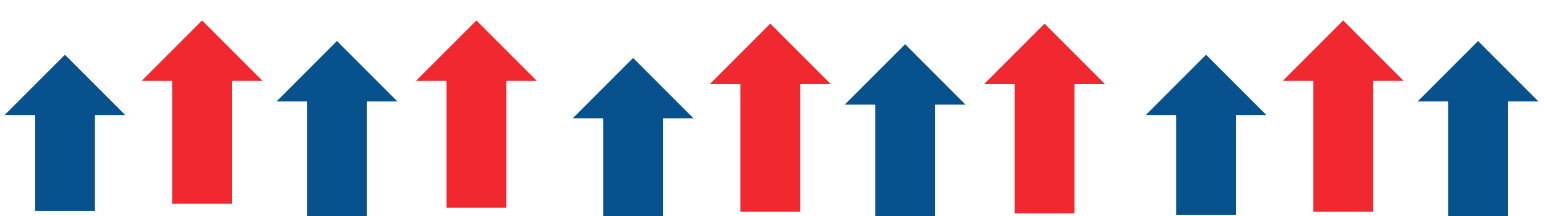
Respostas:

b) A utilização não autorizada das informações pessoais de outra pessoa para cometer fraudes ou outros crimes.

b) Pedidos de informações sensíveis, como palavras-passe ou números de cartões de crédito.

b) Um esquema de investimento que promete rendimentos elevados aos investidores com um risco mínimo.

a) Proteger as contas online, exigindo múltiplas formas de verificação.



a) Pedidos urgentes de informações pessoais ou de ação imediata.

d) Atenuar as vulnerabilidades de segurança e proteger contra as ciberameaças.

a) Rendimentos elevados garantidos com um risco mínimo.

a) Para proteção contra a usurpação de identidade e a ciberperseguição.

Pontuação:

8 respostas corretas: Excelente! Tem uma sólida compreensão dos riscos de segurança comuns e das características das fraudes.

5-7 respostas corretas: Bom trabalho! Tem uma boa compreensão dos conceitos, mas pode beneficiar de uma revisão mais aprofundada.

4 ou menos respostas corretas: Considere a possibilidade de rever o material para melhorar a sua compreensão dos riscos de segurança comuns e das características dos golpes.

COMO COMPRAR ONLINE COM SEGURANÇA

Introdução às compras online

O principal objetivo deste subtópico é familiarizar os alunos com as características e vantagens das compras online. As compras online oferecem uma forma cómoda de fazer compras no conforto de casa. Neste subtópico, os participantes irão explorar vários aspetos dos sites de compras online e percorrer as etapas de compra de um item online - sem concluir a transação. O objetivo aqui é proporcionar uma experiência prática para compreender o processo e as características de fazer uma compra online sem efetuar a transação final.

Navegar nas lojas online

Neste subtópico, o objetivo é aprofundar a compreensão dos alunos sobre as compras online, realçando o aspeto de navegação das lojas online sem a necessidade de efetuar uma compra. A ênfase está em explicar aos alunos que se pode explorar lojas online, ver artigos e

navegar por diferentes categorias sem se comprometer a comprar nada. Isto permite que os indivíduos se habituem ao layout e às características de várias lojas online, compreendam como os produtos são apresentados e como o processo de compra é estruturado. Através da simples navegação, os alunos podem familiarizar-se com a interface do utilizador, as funcionalidades de pesquisa e a experiência geral de compras online sem a pressão de efetuar uma compra. Esta exploração prática é crucial para aumentar a sua confiança e compreensão do ambiente de compras online.

Atividade 1 - Navegar numa loja online.

Os objetivos desta atividade consistem em proporcionar uma experiência prática para os alunos navegarem numa plataforma de compras online e compreenderem os passos essenciais envolvidos na realização de uma compra. Deve começar por instruir os alunos a aceder à Internet e a visitar um sítio Web específico, como a Amazon. Explorando a página inicial e aprendendo a usar as suas características, como a caixa de pesquisa, os separadores de departamento e a navegação através de categorias como "Presentes" e "Livros", os alunos ganharão familiaridade com o layout e as funcionalidades do sítio Web.

A atividade visa ilustrar o processo de refinamento das pesquisas utilizando opções de filtragem e manobrando entre páginas. Além disso, o objetivo principal é clarificar o procedimento passo-a-passo da compra de um artigo online, desde encontrar o artigo até adicioná-lo ao cesto de compras, passando pelo checkout, introduzir os dados de entrega e, por fim, efetuar o pagamento. Este passo-a-passo destina-se a desmistificar e familiarizar os alunos com o processo sequencial de uma compra online, imitando os passos envolvidos numa experiência de compra física.

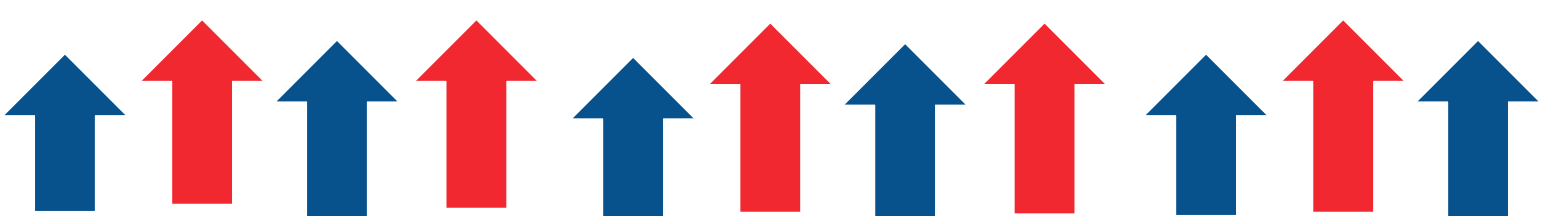
Passo a passo

1. peça ao seu aluno para abrir a Internet.

2. Peça ao seu aprendente para ir a www.amazon.es (ou outro país)

3. Explicar a página inicial da Amazon:

- Caixa de pesquisa.



- Separadores de departamento

4. explorar a página inicial.

5. pedir ao aluno para clicar no separador Presentes e, na categoria de presentes, escolher Livros

6. explorar a página de resultados do livro.

7. explicar que pode utilizar as opções de filtro à esquerda para refinar a sua pesquisa.

8. clicar no botão de retrocesso do browser para voltar à página inicial.

Comprar um artigo online

O objetivo deste subtópico é familiarizar os alunos com as etapas essenciais do processo de compra de artigos através de compras online. A explicação começa por comparar o processo de compra digital com o de uma loja física, dividindo os passos numa sequência simples. Inicialmente, são apresentados aos alunos os passos fundamentais que envolvem encontrar o artigo desejado na loja online, adicioná-lo ao cesto de compras virtual, prosseguir para o checkout, introduzir os detalhes de entrega necessários e concluir a transação efetuando o pagamento. Ao enquadrar o processo de compra online desta forma, o objetivo é simplificar e desmistificar os passos, tornando mais fácil para os alunos compreenderem e navegarem através da experiência de compra online, semelhante às suas rotinas familiares de compras na loja. Esta abordagem estruturada pretende criar confiança e compreensão nos alunos, capacitando-os para se envolverem de forma eficaz e segura nas transações online.

Atividade 2 - Comprar um e-book Kindle Online

O objetivo principal desta atividade é guiar os alunos através dos passos de uma compra online num site de compras, realçando os fatores cruciais para uma experiência de compra online segura e genuína. Os alunos devem ser encaminhados para um sítio Web designado, como a Amazon, onde podem explorar a página inicial enquanto avaliam criticamente a sua autenticidade. Considerações importantes incluem a verificação da existência de um endereço postal, de um número de telefone e de uma política de devoluções visível no sítio.

O processo de compra passo a passo é navegado e apoiado pelo formador que explica cada fase, destacando as principais medidas de segurança, tais como o endereço web que começa por "https", indicando uma transação segura. Os alunos devem ser lembrados de que não estão realmente a fazer uma compra, mas se estivessem, introduziriam os dados de pagamento e receberiam uma confirmação. Além disso, a atividade inclui uma explicação das opções de pagamento como cartão de crédito e PayPal. Após o exercício, os alunos devem ser encorajados a utilizar o botão de retrocesso do navegador para regressar à página inicial, com a advertência de que, ao fazê-lo, apagam todas as informações introduzidas no sítio, reforçando a importância da segurança online e da proteção de dados. Este exercício abrangente tem como objetivo educar os alunos na identificação dos sinais de um site genuíno, compreender o processo de pagamento seguro e enfatizar as práticas de navegação segura durante as experiências de compras online.

Passo a passo

Explique ao seu aluno que ele vai visitar um sítio de compras e seguir os passos para comprar um artigo online, mas que não vai comprar nada.

1. pedir ao aprendente para ir a www.amazon.es (ou outro país)

2. explorar a página inicial - IMPORTANTE:

- O sítio é genuíno?

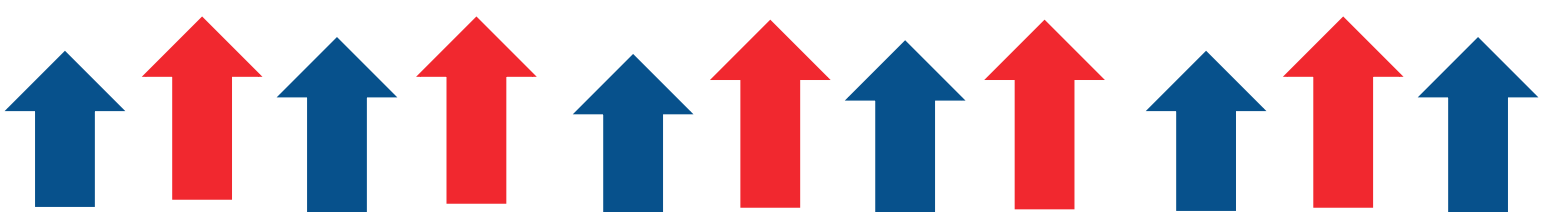
- O sítio apresenta um endereço postal e um número de telefone?

- Têm uma política de devoluções?

Peça ao seu aprendente para seguir os passos de uma compra.

Explique cada passo à medida que avança.

Quando chegarem à página de pagamentos do sítio, peça ao seu aluno para olhar para o endereço Web - deve começar por https - IMPORTANTE Verifique se o endereço Web no navegador começa por https (em vez de http) - isto significa que estão a utilizar algum tipo de segurança ao lidar com o seu dinheiro.



Explique ao seu aluno que, se ele for comprar o artigo, deve agora completar os seus dados de pagamento e receber a confirmação da sua compra. (não o faça!)

Explicar as opções de pagamento.

Cartão de crédito; PayPal

Quando o exercício estiver concluído, peça ao aluno para utilizar o botão de retrocesso do navegador para voltar à página inicial. **Nota:** A utilização do botão de retrocesso do browser irá apagar todas as informações fornecidas no sítio.

Esquemas de romance online

As burlas românticas online são um tipo de cibercrime desonesto e astuto em que os burlões se aproveitam dos laços emocionais das vítimas para lhes roubar dinheiro. Para ganhar a confiança e a proximidade de vítimas crédulas, os burlões adotam frequentemente identidades falsas e parecem estar romanticamente interessados nelas. Estes criminosos utilizam estratégias criativas, como criar histórias cativantes e apresentarem-se como parceiros perfeitos, para levar as vítimas a pensar que estão seguras.

Uma vez criada a confiança, o burlão pode aproveitar-se dos sentimentos da vítima para a coagir a enviar dinheiro ou a revelar dados financeiros ou pessoais sensíveis. Histórias de vida demasiado dramáticas ou impecáveis, relutância em encontrar-se pessoalmente, declarações precipitadas de amor ou devoção e pedidos de ajuda financeira são sinais de alerta de fraude de romance online. Para reduzir a probabilidade de ser vítima destes esquemas fraudulentos, é crucial ter cuidado, ser cético e estar alerta quando se participa em interações online. As fraudes românticas online aproveitam-se das emoções e da confiança das pessoas.

Atividade 3 - Detetar fraudes românticas online

A atividade tem como objetivo educar os participantes sobre a identificação de sinais de alerta de potenciais fraudes nos encontros online. A atividade enfatiza o reconhecimento de sinais de alerta, tais como uma personalidade excessivamente perfeita, evitar encontros presenciais, expressões rápidas de amor e pedidos de ajuda financeira. Além disso, fornece

conselhos de segurança concisos, defendendo a realização de verificações de antecedentes online, abstendo-se de partilhar informações pessoais e confiando nos seus instintos quando se sente desconfortável com uma relação.

A atividade incentiva o debate aberto, permitindo aos participantes fazer e responder a perguntas, ao mesmo tempo que partilham opiniões, preocupações e experiências pessoais ou observadas com esquemas de romance online. Este intercâmbio interativo promove a sensibilização e a preparação contra atividades potencialmente fraudulentas nos encontros online, permitindo que as pessoas naveguem nestas relações de forma mais cautelosa e sensata.

Passo a passo

Discuta alguns sinais vermelhos típicos que podem apontar para uma fraude nos encontros online. Estes podem consistir em:

-Demasiado perfeito para ser verdade: Se a pessoa parecer demasiado perfeita ou se a sua história de vida parecer demasiado dramática, desconfie.

- Evitar encontros presenciais: É um sinal de alerta se a outra pessoa está constantemente a inventar razões para evitar encontrar-se pessoalmente.

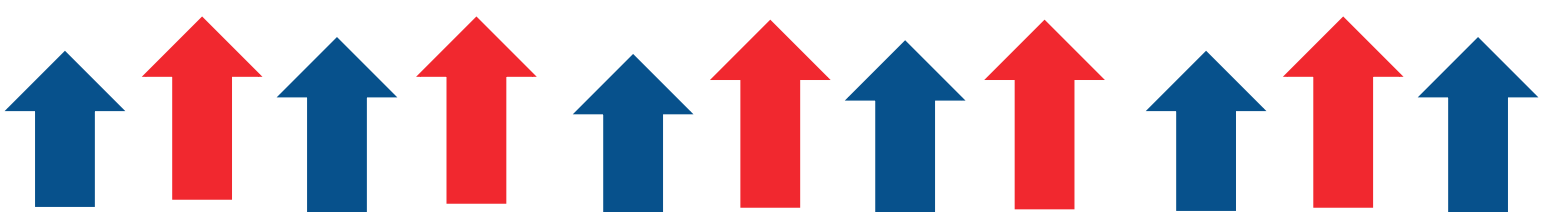
- Declarações de amor rápidas: Pode ser uma pista se eles demonstrarem o seu amor ou devoção muito cedo na relação.

- Pedidos de dinheiro: Nunca dê dinheiro ou divulgue detalhes financeiros a um estranho que não tenha visto pessoalmente.

1) Dar alguns conselhos breves de segurança:

- Efetue sempre um inquérito online sobre o passado de uma pessoa para detetar quaisquer discrepâncias.

Não partilhar informações pessoais: Guarde para si o seu endereço residencial, informações bancárias e número de segurança social.



Se algo lhe parecer estranho, confie nos seus instintos; provavelmente é mesmo assim. Abrace o seu instinto.

2. dar a todos a oportunidade de fazer e responder a perguntas. Incentivar os alunos a discutir as suas opiniões, preocupações e quaisquer experiências pessoais ou observadas com esquemas de romance online.

Atividade 4 - Um vídeo sobre compras seguras

O objetivo desta atividade é orientar os alunos no reconhecimento e implementação de medidas de segurança quando fazem compras online. A atividade deve começar por orientar os alunos para visitarem o site www.getsafeonline.org, navegando depois para a secção "Ver Vídeos" e selecionando o vídeo "Compras Online". Após a conclusão do vídeo, os alunos devem ser instruídos a ir para www.easons.com e avaliar criticamente o site, respondendo a perguntas específicas: se o site apresenta uma política de privacidade e se apresenta um endereço de contacto.

Esta atividade tem como objetivo incentivar os formandos a utilizarem recursos educativos sobre segurança online e a aplicarem os seus conhecimentos na prática, avaliando as medidas de segurança e a transparência de um sítio Web de compras real. Combinando os conhecimentos teóricos do vídeo com uma avaliação prática do sítio Web, os alunos podem discernir e identificar ativamente as precauções de segurança essenciais a ter em conta nas compras online. Este processo facilita uma experiência de aprendizagem prática, reforçando a importância das políticas de privacidade e das informações de contacto para uma experiência de compras online segura.

MÉTODOS DE PAGAMENTO ALTERNATIVOS

Introdução aos métodos de pagamento alternativos

Os métodos de pagamento convencionais, como o numerário e os cartões de crédito, podem ser prejudiciais para a sociedade e o ambiente. Este subtópico aborda esta questão, destacando métodos de pagamento alternativos, tais como:

Carteiras digitais: Ao simplificarem as transações online e ao eliminarem a necessidade de moeda forte e de faturas em papel, estes cartões eletrónicos promovem um sistema financeiro sem papel.

Pagamentos móveis: Para uma vasta gama de serviços e mercadorias, estes serviços, que são executados em dispositivos móveis, assumem o papel dos métodos de pagamento tradicionais, como o dinheiro ou os cartões.

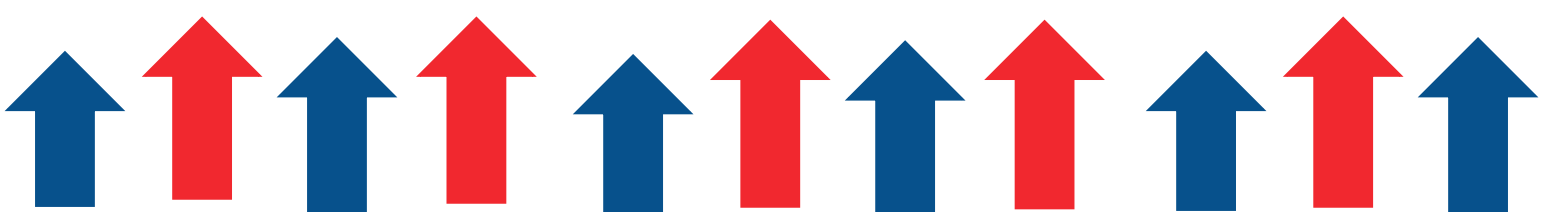
Criptomoedas: Utilizando a tecnologia blockchain, as moedas digitais descentralizadas e seguras permitem transações sem a necessidade de bancos centrais, possivelmente reduzindo a dependência de instituições financeiras estabelecidas.

Os métodos de pagamento alternativos referem-se a formas não tradicionais de efetuar transações financeiras para além do dinheiro ou dos cartões de crédito/débito. Estes métodos ganharam popularidade devido à sua conveniência, acessibilidade e, muitas vezes, à sua integração em plataformas digitais. Cartões pré-pagos, transferências bancárias, carteiras digitais, criptomoedas, programas de fidelização, cartões locais e opções de pagamento adiado são apenas algumas das possibilidades que se enquadram nesta categoria. Devido à sua facilidade de utilização e segurança, a epidemia acelerou ainda mais a sua aceitação.

Impacto no ambiente e na sociedade: A utilização de métodos de pagamento alternativos para transações digitais tem várias vantagens.

Vantagens ecológicas: As transações digitais caracterizam-se por um menor consumo de papel, um menor impacto do carbono e uma melhor eficiência energética. Reduzem os danos que a produção e o trânsito de moeda física causam ao ambiente.

O **impacto das criptomoedas na sociedade** pode ser visto na sua capacidade de reduzir drasticamente os custos de transação, acelerar as transações e incentivar a inclusão financeira, particularmente em comunidades marginalizadas. Isto ajuda a apoiar as economias locais e a fornecer serviços financeiros a pessoas que não têm acesso às instituições tradicionais.



Devido a várias considerações, as transações digitais constituem uma opção mais ecológica do que as transações monetárias tradicionais, que têm, por si só, efeitos ambientais importantes.

Diminuição do impacto ambiental: A produção, a distribuição e a impressão de moeda física têm um rasto substancial de papel que contribui para a perda de árvores. A utilização generalizada de papel-moeda tem efeitos ambientais negativos, como a desflorestação e o aumento das emissões de gases com efeito de estufa. Além disso, o transporte de dinheiro real para os bancos e caixas automáticos aumenta o consumo de combustível e as emissões dos veículos em movimento.

Eficiência energética das transações digitais: Por outro lado, as transações digitais executadas eletronicamente requerem menos energia e equipamento físico substancial. Para reduzir o seu efeito ambiental total, a maioria das transações digitais é tratada em centros de dados alimentados por fontes de energia renováveis. Estas instalações são concebidas para serem tão eficientes quanto possível em termos energéticos, reduzindo significativamente o seu impacto carbónico.

As criptomoedas têm várias vantagens potenciais, especialmente para as populações desfavorecidas que procuram serviços financeiros:

Custos de transação mais baixos: Os bancos e as empresas de remessas cobram frequentemente taxas elevadas pelas transferências internacionais de dinheiro tradicionais. Estas despesas são muito reduzidas pelas criptomoedas, tornando as transferências internacionais de dinheiro mais razoáveis.

Transações mais rápidas: Em comparação com os sistemas bancários normais, as transações em criptomoeda são conhecidas pela sua rapidez. Esta rapidez é particularmente importante para as pessoas que dependem de remessas atempadas para cobrir custos quotidianos ou emergências imprevistas.

Inclusão financeira e economias locais: Ao fornecer serviços financeiros a pessoas sem acesso a instituições bancárias tradicionais, as criptomoedas podem colmatar lacunas

financeiras em locais remotos ou empobrecidos. Esta estratégia inclusiva pode impulsionar significativamente a economia regional e dar mais influência às pessoas desfavorecidas.

Tipos de métodos de pagamento alternativos

Métodos de pagamento alternativos, referem-se a uma variedade de métodos de transação financeira não tradicionais que proporcionam aos clientes mais alternativas para efetuar pagamentos.

Alguns exemplos de métodos de pagamento alternativos são:

Cartões pré-pagos: Estes cartões são pré-carregados com uma determinada quantia de dinheiro e podem ser utilizados para efetuar compras até que o saldo se esgote.

Transferências bancárias: Este método permite aos consumidores pagar bens e serviços online através de transferências diretas online a partir da sua conta bancária.

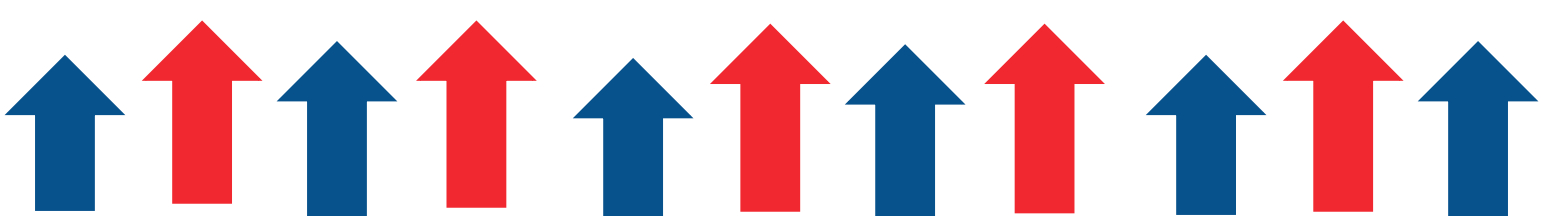
Carteiras digitais: Trata-se de software ou hardware que permite aos utilizadores efetuar pagamentos eletrónicos. Podem ser utilizadas para armazenar vários métodos de pagamento, como cartões de crédito e contas bancárias, e podem ser utilizadas para efetuar compras online ou em lojas.

Criptomoedas: São moedas digitais ou virtuais que utilizam criptografia para segurança e funcionam independentemente de um banco central. Podem ser utilizadas para efetuar compras online ou em lojas que as aceitem como forma de pagamento.

Programas de fidelização: Estes programas permitem aos consumidores ganhar pontos ou recompensas por fazerem compras num determinado retalhista ou marca. Os pontos ou prémios podem depois ser trocados por descontos ou produtos gratuitos.

Cartões locais: Trata-se de cartões de crédito ou de débito emitidos por bancos ou instituições financeiras locais e que só podem ser utilizados num determinado país ou região.

Opções de pagamento diferido e a prestações: Estas opções permitem aos consumidores adiar o pagamento de uma compra ou pagá-la em prestações ao longo do tempo.



Atividade 1: Diferentes tipos de métodos de pagamento alternativos

O principal objetivo desta atividade é fornecer aos alunos um folheto completo que apresenta e explica uma variedade de diferentes opções de pagamento. É fornecida uma breve descrição de cada método, que inclui cartões pré-pagos, transferências bancárias, carteiras digitais, criptomoedas, programas de fidelização, cartões locais e opções de pagamento diferido. O objetivo é fornecer aos alunos uma compreensão básica dos diferentes mecanismos de pagamento, destacando os muitos benefícios, características e situações em que cada abordagem pode ser útil. No final da atividade, os alunos devem ter uma compreensão básica das opções de pagamento alternativas, permitindo-lhes avaliar as possíveis utilizações e vantagens de cada método em várias situações financeiras.

Passo a passo

Distribuir a Folha de Apoio aos alunos.

Pergunte aos alunos se já utilizaram algum destes métodos de pagamento e, em caso afirmativo, como foi a sua experiência.

Atividade 2: Vantagens e desvantagens

O objetivo desta atividade é promover o pensamento crítico e a participação dos participantes na ponderação das vantagens e desvantagens das várias opções de pagamento. No quadro branco ou flipchart, é criada uma área organizada, incentivando a participação numa conversa de grupo. O objetivo do exercício é investigar e compreender as vantagens e desvantagens de várias opções de pagamento alternativas.

Através deste exercício, os alunos podem identificar as vantagens da utilização destas estratégias, incluindo maior flexibilidade, uma base de consumidores mais alargada e possíveis poupanças de custos para as empresas. Ao mesmo tempo, refletem sobre as possíveis desvantagens, tais como a adoção limitada pelas empresas, a necessidade de várias opções de pagamento e os diferentes graus de proteção contra a fraude oferecidos pelas diferentes alternativas. Os alunos compreendem a complexidade dos sistemas de pagamento alternativos e os fatores a ter em conta através desta comparação.

Passo a passo

Peça aos alunos para partilharem as suas ideias sobre as vantagens e desvantagens da utilização de métodos de pagamento alternativos e escreva-as no lado apropriado do quadro (ver exemplos acima).

Utilizar o quadro branco

Guia para um formador: Vantagens e desvantagens

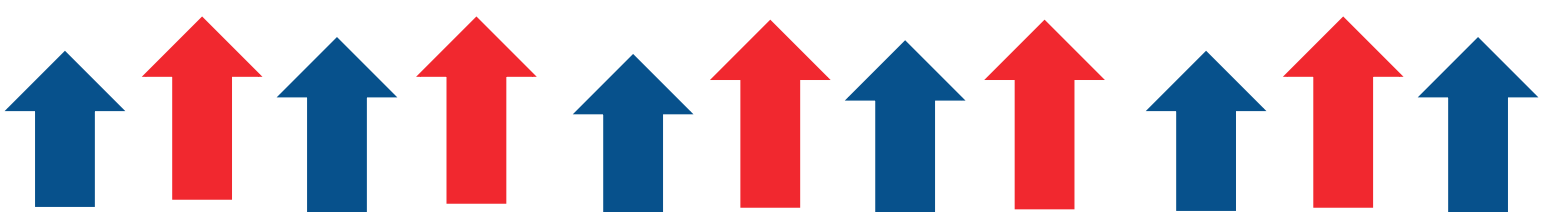
Aspetos como a segurança, a facilidade de utilização, os custos, a disponibilidade e possíveis incentivos são frequentemente objeto de discussões sobre as vantagens e desvantagens de vários sistemas de pagamento alternativos. Ao examinarem cuidadosamente estes fatores, os alunos terão os conhecimentos necessários para equilibrar as vantagens e desvantagens da utilização de métodos de pagamento alternativos. Esta compreensão facilita a tomada de decisões bem informadas relativamente à sua aplicação em diversas transações financeiras.

A utilização de outros métodos de pagamento tem várias vantagens. Para os clientes, quando se trata de fazer compras, proporcionam maior escolha e liberdade. Ao utilizarem o método de pagamento que escolheram, podem também ajudar as empresas a atrair clientes de todo o mundo. Além disso, ao utilizar outras opções de pagamento, as empresas podem reduzir os seus custos de processamento de cartões de crédito.

No entanto, podem existir algumas desvantagens na utilização de opções de pagamento alternativas. Por exemplo, os clientes podem precisar de ter muitas alternativas de pagamento disponíveis, porque nem todas as empresas aceitam todos os tipos de métodos de pagamento alternativos. Além disso, nem todas as outras opções de pagamento oferecem o mesmo grau de proteção contra a fraude que os cartões de crédito.

Atividade 3: Segurança e privacidade da utilização de métodos de pagamento alternativos.

Esta atividade visa abordar as questões de privacidade e segurança associadas à utilização de métodos de pagamento alternativos. Explora os possíveis perigos da utilização de vários métodos de pagamento, incluindo fraude, roubo de identidade e violações de dados. A importância de adotar medidas preventivas para reduzir estes riscos é realçada no debate. Estas medidas preventivas incluem a revisão regular das demonstrações financeiras para



detetar irregularidades, a utilização da autenticação de dois fatores para evitar a apropriação de contas e a garantia de que os destinatários dos pagamentos são legítimos antes de transferir dinheiro. O objetivo é fornecer aos consumidores táticas úteis para reduzir os problemas de segurança e privacidade quando utilizam outros métodos de pagamento.

Passo a passo

Discutir as implicações de segurança e privacidade da utilização de métodos de pagamento alternativos, tais como o risco de fraude, violação de dados e roubo de identidade.

Resuma os principais pontos abordados na aula e sublinhe a importância de utilizar métodos de pagamento alternativos de forma segura e protegida.

Incentive os alunos a colocarem quaisquer questões que possam ter sobre o tema.

Guia para um formador:

A implementação de sistemas de pagamento alternativos depende da preservação da segurança e da privacidade. É fundamental garantir a segurança dessas técnicas para evitar roubos de identidade, fraudes e violações de informações pessoais. É essencial compreender a encriptação e os protocolos de segurança que protegem estas opções de pagamento.

Risco de fraude: Os métodos de pagamento alternativos introduzem novas oportunidades para atividades fraudulentas. Ao contrário dos sistemas de pagamento tradicionais, estes métodos podem ter medidas de segurança menos rigorosas, o que os torna vulneráveis a transações não autorizadas ou a aquisições de contas. Os utilizadores devem ser cautelosos quando partilham as suas informações de pagamento e estar atentos a potenciais tentativas de phishing ou burlas.

Violações de dados: As plataformas de pagamento alternativas armazenam informações financeiras sensíveis, tais como dados de cartões de crédito ou números de contas bancárias. No caso de uma violação de dados, estas informações podem ser comprometidas, levando a perdas financeiras e roubo de identidade. As empresas que oferecem serviços de pagamento alternativos devem dar prioridade a medidas de segurança

robustas para proteger os dados dos utilizadores contra o acesso não autorizado ou ciberataques.

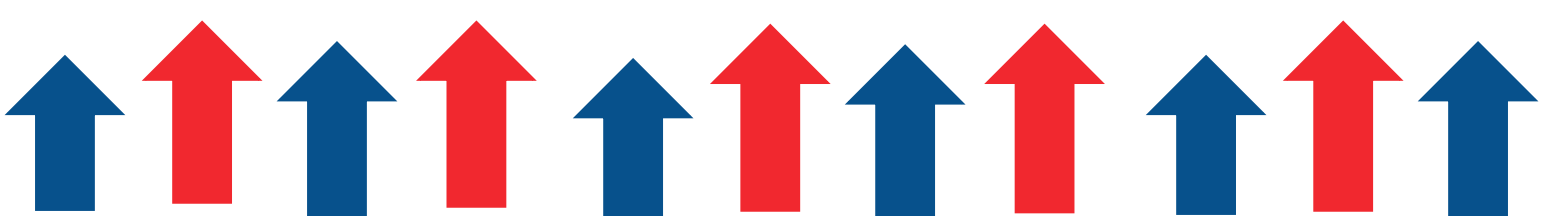
Roubo de identidade: Os métodos de pagamento alternativos aumentam o risco de roubo de identidade, uma vez que exigem frequentemente que os utilizadores forneçam informações pessoais para a criação e verificação da conta. Os cibercriminosos podem explorar as vulnerabilidades destes sistemas para roubar as identidades dos utilizadores e participar em atividades fraudulentas. Os utilizadores devem ter cuidado ao partilhar informações pessoais online e controlar regularmente as suas contas para detetar atividades suspeitas.

Os utilizadores podem reforçar a sua privacidade, tomar decisões informadas e desenvolver confiança na utilização destas tecnologias, conhecendo os procedimentos de segurança e as diretrizes de privacidade associadas a estes modos. O subtópico consiste em dar aos alunos a informação de que necessitam para avaliar as características de segurança e privacidade de várias opções de pagamento alternativas.

Estes métodos de pagamento proporcionam aos clientes mais escolhas e flexibilidade ao efetuarem compras, mas existe a possibilidade de ocorrerem fraudes, roubo de identidade e violações de dados.

As opções de pagamento alternativas podem ter efeitos na privacidade e na segurança. Estes métodos de pagamento proporcionam aos clientes mais escolhas e flexibilidade ao efetuarem compras, mas existe a possibilidade de ocorrerem fraudes, roubos de identidade e violações de dados.

Ao utilizar métodos de pagamento alternativos, os consumidores podem adotar algumas medidas de segurança para reduzir estes perigos. Por exemplo, devem auditar periodicamente as suas demonstrações financeiras para descobrir quaisquer irregularidades. Além disso, para se protegerem contra a aquisição de contas que pode resultar em fraude nos pagamentos, têm de ativar a autenticação de dois fatores. Antes de enviar dinheiro, os clientes devem também confirmar o destino do seu pagamento.



CONCLUSÃO

Este módulo proporcionou aos participantes conhecimentos essenciais e competências práticas em matéria de segurança online e literacia financeira. Ao explorar temas como os riscos de segurança online, as compras online seguras e os métodos de pagamento alternativos, os participantes adquiriram conhecimentos sobre a proteção eficaz das informações pessoais e financeiras. O módulo visa capacitar os indivíduos para tomarem decisões informadas e adotarem práticas financeiras seguras e sustentáveis na era digital atual.

REFERÊNCIAS

Grupo de Trabalho Anti-Phishing (APWG). (n.d.). Recuperado de https://www.apwg.org/

Agência para a Cibersegurança e a Segurança das Infra-estruturas (CISA). (n.d.). Recuperado de https://www.cisa.gov/

Comissão Federal do Comércio (FTC). (n.d.). Recuperado de https://www.ftc.gov/

Grigutytė, M., & Grigutytė, M. (2023, 27 de dezembro). Golpe do Príncipe Nigeriano: o que é e como funciona. NordVPN. https://nordvpn.com/pt/blog/nigerian-prince-scam/

Hayes, A. (2023, 20 de dezembro). Bernie Madoff: Quem ele era, como funcionava seu esquema Ponzi. Investopedia. https://www.investopedia.com/terms/b/bernard-madoff.asp

Better Business Bureau. (2021). Como se proteger nas compras online. https://www.bbb.org/article/tips/11205-bbb-tip-how-to-protect-yourself-when-shopping-online

Planos de aula de ESL | Your English Pal. (2022, 3 de fevereiro). Your English Pal. https://www.yourenglishpal.com

Comissão Federal do Comércio. (2021). Dicas de compras online. https://www.consumer.ftc.gov/articles/online-shopping-tips

Get Safe Online | O principal recurso de aconselhamento sobre segurança online do Reino Unido. (2023, 1 de novembro). Get Safe Online. https://www.getsafeonline.org/)

Kaspersky. (2021). Compras online seguras: 10 dicas para evitar fraudes. https://www.kaspersky.com/resource-center/online-safety/safe-online-shopping

Norton. (2021). Dicas de segurança para compras online: Como fazer compras online com segurança. https://us.norton.com/internetsecurity-online-shopping-safety-tips-how-to-shop-online-safely.html

Jackson, W. (2023, 10 de julho). William Jackson | Políticas de segurança de dados: Necessárias mas não suficientes. Route Fifty. https://www.route-fifty.com/cybersecurity/2007/12/william-jackson-data-security-policies-necessary-but-not-sufficient/308532/

K. (2023, 10 de março). Mantendo seu dinheiro seguro online. YouTube. https://www.youtube.com/watch?v=EL0_zRfpEnQ

Marsh, L. (2023, 3 de novembro). Como evitar fraudes de pagamento como gerente de propriedade. Forbes. https://www.forbes.com/sites/forbescommunicationscouncil/2023/11/03/how-to-avoid-payment-fraud-as-a-property-manager/?sh=455340a03362

Mileva, G. (2023, 26 de outubro). Tudo o que você precisa saber sobre métodos de pagamento alternativos em 2024. Centro de marketing de influência. https://influencermarketinghub.com/alternative-payment-methods/

Solução de processamento de pagamentos online. (n.d.). GoCardless. https://gocardless.com/

Payne, K. (2023, 18 de julho). Revisão do Banco Axos. Investopedia. https://www.investopedia.com/axos-bank-review-4802090

Quais são os riscos dos pagamentos digitais? (2020, 5 de fevereiro). Fórum Económico Mundial. https://www.weforum.org/agenda/2015/02/what-are-the-risks-of-digital-payments/

FinPower

Cofinanciado pela União Europeia

Financiado pela União Europeia. Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidos como responsáveis por essas opiniões. Número do Projeto: 2022-1-AT01-KA220-ADU-000087985