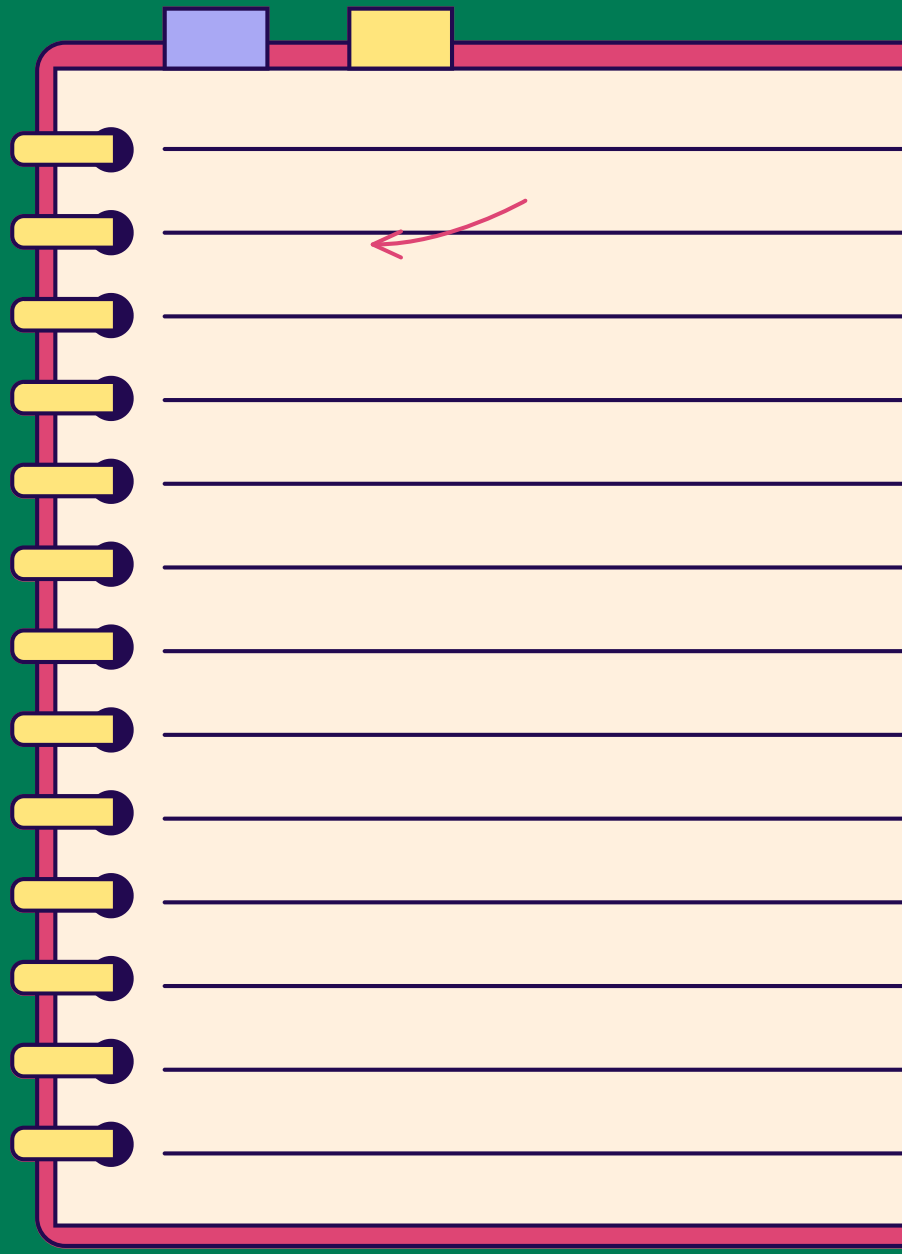
MÓDULO 12 - GOLPES ONLINE

CAPÍTULO 3

COMO REAGIR A BURLAS

Skills to Connect



INTRODUÇÃO

Neste capítulo, aprenderá a reagir a várias situações de fraude online, quer tenha clicado numa hiperligação fraudulenta, quer tenha sido vítima de spoofing (roubo de identidade) ou de fraude na compra. Vamos guiá-lo através das acções que deve tomar imediatamente para proteger as suas contas, comunicar o incidente e evitar outras consequências nefastas.

Também descobrirá os websites oficiais para denunciar fraudes em diferentes países e as melhores práticas a adotar para proteger as suas informações pessoais a partir de agora.

1 COMO REAGIR A GOLPES

O QUE FAZER QUANDO SE CLICA NUMA HIPERLIGAÇÃO FRAUDULENTA

CLICOU NUMA LIGAÇÃO FRAUDULENTA APÓS UMA TENTATIVA DE PHISHING: O QUE DEVE FAZER AGORA?

1 - NÃO INSIRA NENHUM DADO

- Se introduzir os seus dados de acesso num site falso, estará a dar ao cibercriminoso acesso direto à sua conta real. Uma vez iniciada a sessão, ele poderá utilizar a sua conta para fins maliciosos. A situação torna-se ainda mais grave se reutilizar a mesma senha em várias contas, uma vez que isso lhe dará acesso a essas outras contas também.

2 - NÃO CLIQUE EM NADA

- Se entrar num site suspeito, não clique nas ligações, pois podem conter vírus prontos a serem activados. Evite também clicar em anúncios: estes podem conter software malicioso, um fenómeno conhecido como “malvertising”. Mesmo um simples clique pode desencadear a instalação de um programa nocivo no seu dispositivo.

3 - INTERROMPA A LIGAÇÃO À INTERNET E MUDE AS SUAS SENHAS

- Cortar a sua ligação à Internet bloqueia o acesso remoto ao seu dispositivo por parte do cibercriminoso. Também limita a propagação de software malicioso a outros dispositivos ligados à sua rede Wi-Fi. Desligar rapidamente o dispositivo pode reduzir consideravelmente o risco de danos.
- Assim que o dispositivo for desconectado, utilize outro dispositivo fiável (como outro computador, tablet ou smartphone) para mudar as suas senhas.
  - Conecte-se a uma rede segura: evite redes Wi-Fi públicas. Utilize a sua rede doméstica ou partilhe a ligação à Internet de um smartphone (modo “partilha de ligação” ou “hotspot móvel”).
  - Aceda a sites importantes, como o seu correio eletrónico, contas bancárias ou redes sociais.
  - Clique em “Esqueceu-se da sua palavra-passe?” se tiver problemas em iniciar sessão. Isto permitirá que redefina a senha seguindo as instruções enviadas por e-mail ou SMS.

1 COMO REAGIR A GOLPES

O QUE FAZER QUANDO SE CLICA NUMA HIPERLIGAÇÃO FRAUDULENTA

4 - FAÇA UMA VERIFICAÇÃO COMPLETA COM O ANTIVÍRUS:

- Após a desconexão, é importante analisar o dispositivo com software antivírus. Se ainda não tiver instalado um, faça-o sem demora. O software antivírus analisa o seu dispositivo para detetar e remover vírus ou malware antes que estes causem danos graves. Para o fazer:
  - Abra o antivírus instalado no seu dispositivo.
  - Escolha a opção “Análise completa” ou “ Verificação completa”. Isto permite que o antivírus examine todos os ficheiros no seu computador, incluindo as áreas sensíveis onde os vírus se escondem frequentemente.
  - Quando a verificação estiver terminada, siga as recomendações do antivírus: elimine ou coloque em quarentena todas as ameaças detectadas.
  - Após a verificação, volte a estabelecer ligação apenas se o seu dispositivo estiver limpo (sem ameaças detectadas).
  - Uma vez conectado, actualize o seu antivírus para que este tenha a proteção mais recente contra novas ameaças. Depois, efectue outra verificação para confirmar que tudo esteja seguro.

5 - CONTROLE AS SUAS CONTAS:

- Mesmo depois de tomar estas precauções, mantenha-se vigilante, monitorizando regularmente as suas contas para detetar qualquer atividade suspeita. O cibercriminoso pode ter tido tempo para recuperar informações sensíveis. Verifique com atenção os seus extractos bancários para detetar transacções que não efectuou, bem como inícios de sessão fora do habitual ou alterações não autorizadas nas suas contas electrónicas.

2 COMO REAGIR A GOLPES

O QUE FAZER SE FOR VÍTIMA DE SPOOFING

ALGUÉM FINGIU SER O SEU BANQUEIRO E ROUBOU-LHE DINHEIRO: O QUE DEVE FAZER AGORA?

1 - CONTACTE IMEDIATAMENTE O SEU BANCO

- Telefone para o seu banco utilizando o número oficial (o que está impresso no seu cartão bancário ou no website oficial). Explique o que aconteceu e peça-lhes que :
  - Bloqueiem os seus cartões bancários se tiver fornecido os seus números,
  - Verifiquem as suas contas para bloquear quaisquer transacções suspeitas,
  - Modifiquem o acesso às suas contas online para evitar que o fraudador inicie sessão.

2 - MUDE AS SUAS SENHAS

- Altere imediatamente as senhas de todas as suas contas sensíveis, especialmente :
  - As suas contas bancárias digitais,
  - A sua caixa de correio eletrónico (pois é frequentemente utilizada para recuperar senhas),
  - As suas contas noutros serviços (redes sociais, sites de compras) se usa a mesma senha.

2 COMO REAGIR A GOLPES

O QUE FAZER SE FOR VÍTIMA DE SPOOFING

3 - MONITORE AS SUAS CONTAS BANCÁRIAS

- Verifique os seus extractos bancários e transacções online para detetar pagamentos ou transferências que lhe tenham escapado.
  - Active as notificações por SMS ou e-mail para ser alertado assim que uma transação for realizada.
  - Se detetar quaisquer transacções suspeitas, comunique-as imediatamente ao seu banco.

4 - APRESENTE UMA QUEIXA

- Dirija-se à esquadra da polícia para apresentar queixa. Leve todas as provas que puder: o número que o contactou, mensagens, e-mails ou capturas de ecrã relacionadas com a burla.
- Também pode denunciar a burla online em plataformas específicas:
  - Em França: Denuncie através da plataforma Pharos
  - Na Bélgica: Denuncie na Safeonweb.be
  - Em Portugal: Apresente uma queixa à Polícia de Segurança Pública (https://www.policiajudiciaria.pt/queixa-eletronica/) ou ao Gabinete de Combate ao Cibercrime (https://cibercrime.ministeriopublico.pt/pagina/denuncia-0)

3 COMO REAGIR A GOLPES

O QUE FAZER SE FOR VÍTIMA DE FRAUDE NAS COMPRAS

FEZ UMA COMPRA NUM SITE FRAUDULENTO: O QUE DEVE FAZER AGORA?

1 - CONTACTE IMEDIATAMENTE O SEU BANCO OU O OPERADOR DO CARTÃO

- Se pagou com cartão bancário ou outro meio de pagamento, contacte imediatamente o seu banco ou o fornecedor do cartão. Explique a situação e peça para :
  - Cancelar a transação, se possível,
  - Suspender o débito no seu cartão para evitar novos pagamentos fraudulentos,
  - Verificar se houve pagamentos não autorizados noutras transacções recentes.

2. MUDE AS SUAS SENHAS

- Se introduziu informações sensíveis (como a sua senha ou dados bancários) no site fraudulento, altere as senhas das suas contas bancárias online, da sua caixa de correio eletrónico e de quaisquer outras contas utilizadas com essa senha.

3 COMO REAGIR A GOLPES

O QUE FAZER SE FOR VÍTIMA DE FRAUDE NAS COMPRAS

3 - MONITORE AS SUAS CONTAS

- Verifique os seus extractos bancários e esteja atento a qualquer atividade suspeita, especialmente se estiverem a ocorrer transacções não autorizadas.
- Active o serviço de alertas por SMS ou e-mail do seu banco para ser informado em tempo real de qualquer atividade nas suas contas.
- Verifique também as suas contas online (Amazon, PayPal, etc.) para se certificar de que nenhuma informação foi utilizada de forma fraudulenta.

4 - DENUNCIE O SITE FRAUDULENTO

- Apresente uma queixa à polícia local ou online.
- Também pode denunciar a burla online em plataformas específicas:
  - Em França: Denuncie através da plataforma Pharos
  - Na Bélgica: Denuncie em Safeonweb.be
  - Em Portugal: Denuncie em https://queixaselectronicas.mai.gov.pt/
- Pode também denunciar o site fraudulento às organizações de consumidores:
  - Trustpilot
  - Signal-Arnaques
  - ScamDoc

4 O QUE DEVE FAZER SE DETETAR UMA BURLA?

PLATAFORMAS DE DENÚNCIA E PREVENÇÃO

BÉLGICA

- Cybersimple.be: esta plataforma oferece conselhos sobre a prevenção de burlas online, fornecendo informações sobre tipos comuns de fraudes e a comunicação de incidentes de cibersegurança.
- Centre pour la Cybersécurité Belgique: O centro de cibersegurança belga (CCB) ajuda a assinalar incidentes de cibersegurança, incluindo ataques de phishing, e dá conselhos sobre como proteger o seu dispositivo.
- Safe On Web: Plataforma oficial para denunciar burlas e incidentes de cibersegurança. Também fornece recomendações relativas à proteção contra riscos digitais.

FRANÇA

- Thesee: Plataforma oficial do Ministério do Interior para denunciar burlas na Internet (phishing, fraude bancária, etc.). Também é possível apresentar queixas.
- Cybermalveillance: Plataforma para denunciar ciberataques e obter ajuda em caso de incidentes de cibersegurança. Este site oferece conselhos e recursos para as vítimas.
- Pharos: Plataforma oficial para denunciar conteúdos ilegais online (burlas, phishing, cibercrime). Permite denunciar fraudes electrónicas às autoridades competentes.

4 O QUE DEVE FAZER SE DETETAR UMA BURLA?

PLATAFORMAS DE DENÚNCIA E PREVENÇÃO

PORTUGAL

- Seguranet: Site do governo português que fornece informações sobre como denunciar fraudes na Internet e conselhos acerca de proteção contra ataques informáticos e phishing.

UNIÃO EUROPEIA

- Site da UE - Direitos das vítimas: Este site europeu fornece informações sobre os direitos das vítimas de crimes em toda a UE, incluindo a forma de denunciar fraudes e crimes transfronteiriços.

PARA LEMBRAR !

Se for vítima de uma burla online, aja rapidamente, alterando as suas senhas, contactando o seu banco e comunicando o incidente às autoridades competentes. É essencial não clicar em quaisquer novas hiperligações e desconectar o seu dispositivo da Internet para evitar a propagação de software malicioso. Se monitorizar regularmente as suas contas e utilizar ferramentas de segurança como um software antivírus e a autenticação de dois factores, pode limitar os riscos e proteger as suas informações pessoais. Por último, mantenha-se alerta para futuras tentativas de burla, aprendendo a reconhecer os sinais de uma burla.