COMPROMETIMENTO DE E-MAIL DE CEO/NEGÓCIO (CMN)

A fraude de CEO/CMN acontece quando um funcionário de uma empresa é enganado de modo a pagar uma fatura falsa ou a fazer uma transferência não autorizada com a conta da empresa.

COMO FUNCIONA?

O atacante liga ou manda um e-mail fingindo ser um quadro importante da empresa (CEO, etc).

Manifesta bom conhecimento da empresa.

Requer um pagamento urgente.

Usa termos como "Confidencial", "A empresa confia em si", "Estou indisponível de momento".

Refere uma situação sensível (impostos, fusões, aquisições).

É ordenado ao funcionário que não siga os procedimentos normais de autorização.

Instruções de como proceder são enviadas mais tarde, por outra pessoa ou por e-mail.

O funcionário transfere os fundos para uma conta controlada pelo atacante.

Com frequência, é pedido um pagamento internacional para fora da Europa.

QUAIS OS SINAIS?

- E-mail/chamada não solicitada
- Contacto direto de um quadro superior com o qual normamente não fala
- Pedido de confidencialidade absoluta
- Pressão e pedido de urgência
- Pedido estranho, em contradição com os procedimentos internos
- Ameaças, elogios ou promessas de recompensa

O QUE PODE FAZER?

COMO EMPRESA

Estar atenta aos riscos e assegurar que os **funcionários estão informados e atentos.**

Incentivar os funcionários a terem **cuidado especial com os pagamentos.**

Implementar protocolos internos para pagamentos.

Implementar procedimentos para verificar a legitimidade de pagamentos pedidos por mail.

Estabelecer **rotinas de reporte** para gestão de fraude.

Rever a informação no site da empresa, **restringindo a informação e mostrando prudência** nas redes sociais.

Melhorar e atualizar a segurança técnica.

! Contactar sempre a polícia em casos de tentativas de fraude, mesmo que não tenham tido sucesso.

COMO FUNCIONÁRIO

Aplicar com rigor os procedimentos de segurança em pagamentos e encomendas. **Não ignorar passos necessários nem ceder à pressão.**

Verificar sempre cuidadosamente endereços de e-mail relativos a informação sensível/pagamentos.

Em caso de dúvida sobre um pagamento, **consultar um superior.**

Nunca abra links ou anexos suspeitos recebidos por e-mail. Tenha particular cuidado quando aceder a e-mails pessoais em computadores da empresa.

Limite a informação e tenha cautela com o que partilha em redes sociais.

Não partilhe informação sobre a hierarquia da empresa, procedimentos e segurança.

! Se receber e-mails ou chamadas suspeitas, informe a área de segurança ou o departamento de informática.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · Polícia Judiciária · APB Associação Portuguesa de Bancos

#CyberScams

FRAUDES DE INVESTIMENTO

As fraudes de investimento mais comuns incluem, por exemplo, propostas de oportunidades lucrativas de investimento em ações, criptomoedas, metais raros, terrenos ou energias alternativas.

QUAIS OS SINAIS?

- São prometidos lucros rápidos e assegurada a segurança do investimento.
- A oferta só está disponível por tempo curto.
- Recebe repetidas chamadas de números desconhecidos.
- É dito que a oferta é só para si e pedido que não a partilhe.

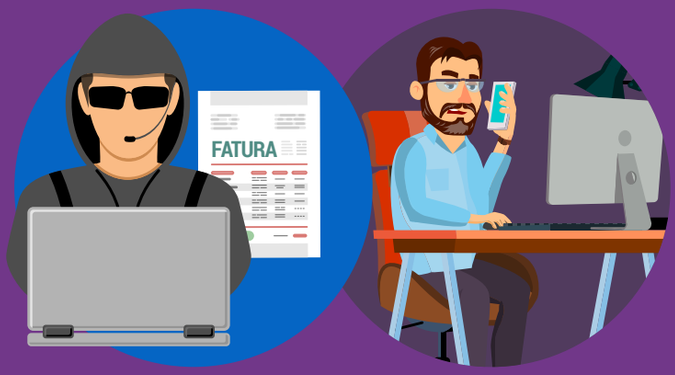
O QUE PODE FAZER?

- **Obtenha sempre aconselhamento imparcial** antes de enviar dinheiro ou fazer investimentos.
- **Rejeite chamadas desconhecidas** sobre investimentos.
- **Desconfie** de ofertas prometendo investimento seguro, retorno garantido e lucros elevados.
- **Esteja atento a esquemas futuros.** Se já foi alvo antes, é provável que os criminosos voltem a tentar ou vendam os seus dados a outros criminosos.
- **Contacte a polícia** se tiver suspeitas.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams

FRAUDE DE FATURAS



COMO FUNCIONA?

- Uma empresa é contactada por alguém que se diz representar um fornecedor/credor.
- Podem ser usados vários meios em simultâneo: telefone, carta, e-mail, etc.
- O atacante pede que os dados do banco para pagamento (ex: dados da conta bancária) de futuras faturas sejam alterados. A nova conta é controlada pelo atacante.

O QUE PODE FAZER?

COMO EMPRESA

Garanta que os **funcionários estão atentos e informados** para esta fraude e como a evitar.

Garanta que os funcionários que fazem pagamentos de faturas **verificam eventuais irregularidades**.

Crie **processos para verificar** a legitimidade de pedidos de pagamento.

Reveja os dados apresentados no seu site, no que respeita a contratos e fornecedores. Garanta que os seus colaboradores não partilham dados da empresa nas redes sociais.

COMO EMPREGADO

Verifique todos os pedidos que dizem ser provenientes dos seus credores, especialmente se pedem alterações nos dados bancários.

Para pagamentos de montantes mais elevados, crie um **procedimento para confirmação** da conta e beneficiário (ex: uma reunião com a empresa).

Não use os contactos indicados na carta/fax/e-mail com o pedido. Use os que tiver recolhido em **comunicações anteriores**.

Quando uma fatura é paga, **envie um e-mail para o beneficiário**. Inclua o nome do banco do beneficiário e os últimos 4 dígitos da conta destino para reforçar a segurança.

Identifique claramente **Pontos Únicos de Contacto** com as companhias para as quais faz pagamentos.

Reduza a informação que partilha sobre a sua empresa nas redes sociais.

Reporte sempre à polícia tentativas de fraude, mesmo que não tenha sido afetado por elas.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams

FRAUDE EM COMPRAS ONLINE

Oportunidades online podem ser atrativas, mas esteja atento.

O QUE PODE FAZER?

- **Use sites de compras nacionais** quando possível - será mais facil resolver eventuais problemas.
- **Pesquise** - veja as avaliações e comentários antes de comprar.
- **Use cartões de crédito** - tem mais chances de receber o dinheiro de volta.

- **Pague apenas com serviços de pagamento seguros** - pedem-lhe pagamentos em dinheiro ou por transferência? Pense duas vezes!
- Pague apenas quando ligado a uma **comunicação de internet segura** - evite redes wifi públicas.
- **Pague apenas num equipamento seguro** - mantenha o seu software sempre atualizado.
- Tenha cuidado com ofertas de descontos ou produtos "miraculosos" - **Se parece bom demais, provavelmente é!**
- Uma janela “pop-up” a dizer que ganhou um prémio? **Pense duas vezes.** Pode ganhar um vírus.
- Se o produto não chegar, contacte o vendedor. Se não tiver resposta, **contacte o seu banco**.

Reporte sempre à polícia tentativas de fraude, mesmo que não tenha sido afetado por elas.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams

E-MAILS DE PHISHING

O phishing usa e-mails fraudulentos para enganar o destinatário de modo a que este partilhe dados pessoais, financeiros ou códigos de segurança.

COMO FUNCIONA?

Estes e-mails:

podem parecer idênticos ao tipo de correspondência enviada pelos bancos.

copiam logótipos, estilo visual e mensagens de e-mails reais.

pedem para descarregar um anexo ao e-mail ou clicar num link.

usam linguagem para transmitir urgência.

O QUE PODE FAZER?

- **Mantenha o seu software atualizado,** incluindo browser, antivírus e sistema operativo.
- Esteja **especialmente atento** se um suposto e-mail do banco lhe pedir dados sensíveis (ex: os códigos de acesso ao homebanking).
- **Examine o e-mail com cuidado:** compare o endereço com o de mensagens anteriores do banco. Veja se encontra erros de escrita.
- **Não responda a e-mails suspeitos.** Encaminhe-os para o seu banco escrevendo o endereço manualmente.
- **Não clique nos links nem descarregue ou abra os anexos.** Escreva manualmente o endereço do seu banco no browser.
- Em caso de dúvida, **verifique a autenticidade** no site do banco ou por telefone.

Os atacantes confiam que as pessoas não estão atentas; numa vista rápida, estes e-mails falsos parecem verdadeiros.

#CyberScams

Atenção quando usa o seu telemóvel. Pode ser mais difícil detetar uma tentativa de ataque no telemóvel ou no tablet.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

FRAUDE DE ROMANCE

Os piratas atacam vítimas em sites de encontros, redes sociais ou enviando e-mails para estabelecer contacto.

QUAIS OS SINAIS?

Alguém que conheceu recentemente online diz ter sentimentos por si e pede uma conversa privada.

As mensagens que enviam são vagas ou mal escritas.

O seu perfil online não está de acordo com o que lhe dizem.

Podem pedir-lhe para mandar imagens ou vídeos íntimos seus.

Primeiro, ganham a sua confiança. Depois, pedem dinheiro, presentes, dados da sua conta ou cartões.

Se não mandar dinheiro podem tentar a chantagem. Se mandar, vão pedir mais.

FOI VÍTIMA?

Não sinta vergonha.
Pare os contactos de imediato.
Se possível, guarde as comunicações feitas, como as mensagens de chat.
Faça queixa à polícia.
Reporte a situação no site onde o pirata o contactou inicialmente.
Se forneceu dados de conta ou cartão, contacte o seu banco.

O QUE PODE FAZER?

- **Tenha muito cuidado** com os dados pessoais que mostra em redes sociais ou sites de encontros.
- **Avalie sempre os riscos.** Os piratas aparecem também nos sites mais fiáveis.
- **Vá devagar** e faça perguntas.
- **Pesquise** online a foto e o perfil da pessoa para ver se já foram usados noutros locais.
- **Esteja atento** a erros de escrita, dados estranhos nas histórias da pessoa ou desculpas, como dizer que a câmera não funciona.
- **Nunca partilhe** material comprometedor que possa ser usado contra si.
- Se combinar um encontro pessoal, **diga à sua familia e amigos** onde vai.
- **Desconfie de pedidos de dinheiro.** Nunca envie dinheiro ou dados de cartões de crédito, contas ou cópias de documentos pessoais.
- **Evite fazer pagamentos à cabeça.**
- **Não transfira dinheiro a pedido de outra pessoa:** a lavagem de dinheiro é crime.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams

SMSs DE PHISHING

O “smishing” (combinação das palavras SMS e Phishing) é a tentativa por atacantes de obter dados pessoais, financeiros ou de segurança por mensagem de texto.

COMO FUNCIONA?

A mensagem de texto tipicamente pedirá para clicar num link ou ligar para um número de modo a "verificar", “atualizar", ou "reativar" a sua conta. Mas... o link leva a uma página falsa e o número de telefone liga ao atacante, que finge ser a empresa verdadeira.

O QUE PODE FAZER?

- **Não carregue em links, anexos ou imagens** que receba em mensagens de texto não solicitadas, sem verificar quem as mandou.
- **Não deixe que o apressem**. Verifique calmamente tudo o que precisa antes de responder.
- **Nunca responda a mensagens de texto** que lhe peçam o PIN, passwords de acesso ao banco ou outros códigos de segurança.
- Se acha que respondeu a uma mensagem de smishing, indicando dados bancários, **contacte o seu banco imediatamente**.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams

SITES BANCÁRIOS FALSOS

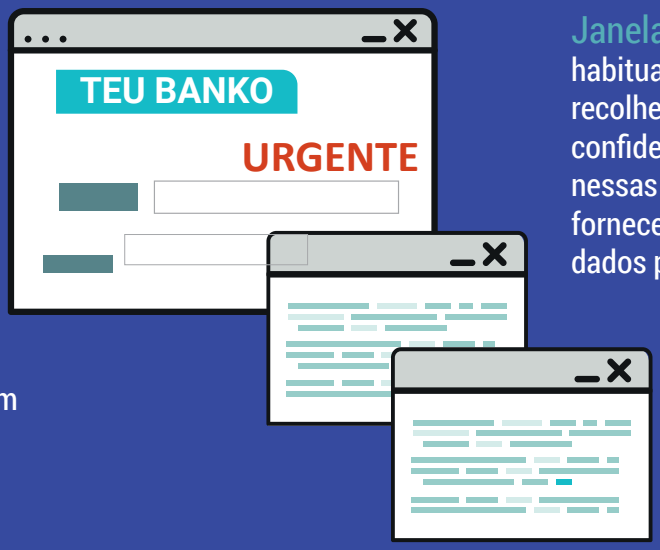
E-mails de phishing bancário habitualmente contêm links que o levam a páginas falsas, onde lhe pedem que divulgue dados financeiros e/ou pessoais.

QUAIS OS SINAIS?

Os sites bancários falsos são parecidos com os originais legítimos. Frequentemente apresentam janelas "pop-up" onde lhe são pedidos os seus dados de acesso. Os bancos não usam páginas semelhantes.

As páginas falsas, em geral, apresentam:

Urgência: não encontrará mensagens assim nos sites verdadeiros.



Janelas "pop-up": são habitualmente usadas para recolher os seus dados confidenciais. Não clique nessas janelas e evite fornecer nelas quaisquer dados pessoais.

Mau design: tenha cuidado com sites que apresentam falhas no design ou erros de escrita.

O QUE PODE FAZER?

Não carregue em links em e-mails que parecem apontar para o site do banco.

Escreva sempre o link manualmente ou use um link guardado nos seus favoritos.

Use um browser que permita **bloquear janelas "pop-up".**

Se algo importante precisar da sua atenção, será alertado para isso pelo seu banco, **após o acesso online à sua conta.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLÍCIA JUDICIÁRIA | APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams

CHAMADAS DE VISHING

O vishing (combinação das palavras voice e phishing) é um ataque por telefone no qual o atacante tenta enganar a vítima para que esta forneça dados pessoais, financeiros ou de segurança ou transfira dinheiro para ele.

O QUE PODE FAZER?

- **Tenha cuidado** com chamadas não solicitadas.
- **Anote o número de quem liga** e indique-lhe que vai ligar de volta.
- Para verificar a identidade de quem liga, **procure o número de telefone da entidade** e ligue diretamente para lá.
- **Não valide quem lhe liga usando o número de telefone que essa pessoa lhe deu** (pode ser falso ou mascarado).
- Os atacantes podem encontrar os seus dados básicos online (redes sociais, p.ex.). **Não assuma que a chamada é genuína** porque têm esses dados.
- **Não partilhe** o PIN do cartão de crédito ou débito nem a password do seu homebanking. O seu banco não lhe pede esses dados.
- **Não transfira dinheiro** para outra conta a pedido de quem lhe liga. O seu banco nunca lho pedirá.
- Se acha que a chamada é falsa, **reporte-o ao seu banco.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

POLÍCIA JUDICIÁRIA

APB ASSOCIAÇÃO PORTUGUESA DE BANCOS

#CyberScams