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