CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

CEO FRAUD

BUSINESS EMAIL COMPROMISE FRAUD

O **CENTRO NACIONAL DE CIBERSEGURANÇA (CNCS)** CHAMA A ATENÇÃO PARA AS SEGUINTES **METODOLOGIAS DE ATAQUE** E **BOAS PRÁTICAS DE PREVENÇÃO**.

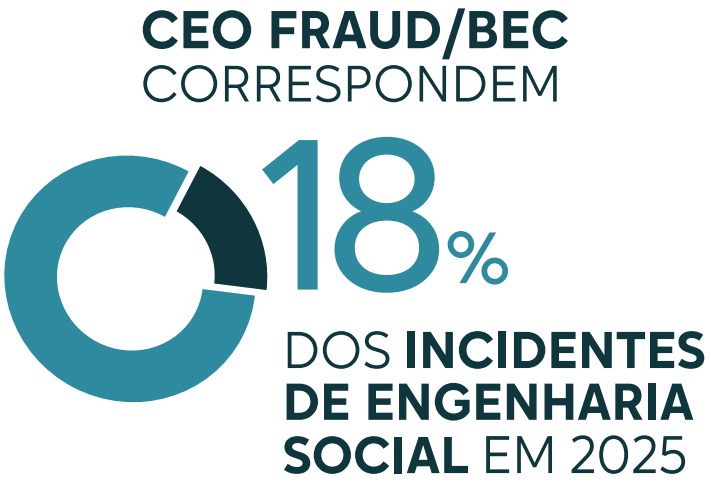
ENQUADRAMENTO

Nos últimos meses, tem sido registado um crescente número de casos de ***CEO Fraud*** e de ***Business Email Compromise Fraud*** **(BEC)**. Este tipo de incidente tem afetado cidadãos e organizações e pode resultar em perdas financeiras significativas.

As campanhas de *CEO Fraud*/BEC caracterizam-se, essencialmente, pelo envio de emails ou mensagens de texto (SMS ou através de aplicações) em que um agente malicioso, fazendo-se passar por uma entidade ligada à organização alvo (por exemplo, o/a Diretor(a) Executivo(a) ou um fornecedor), faz pedidos tipicamente de natureza financeira a colaboradores dessa mesma organização, invocando, por vezes, o carácter urgente ou reservado do pedido, podendo conduzi-los a realizar transferências bancárias para contas associadas ao atacante.

Destacam-se, em particular, campanhas onde o agente malicioso, em mensagens de texto ou *emails* direcionados a colaboradores, se faz passar pelo(a) Diretor(a) Executivo(a) da entidade alvo, ou por fornecedores desta mesma entidade. Nestas comunicações, o atacante solicita a **alteração de dados bancários** relacionados com pagamentos correntes de modo a desviar os mesmos para contas bancárias sob o seu controlo. Nalguns casos são apresentados ficheiros comprovativos, maioritariamente documentos forjados, de alteração de contas bancárias.

Para proteger uma organização deste tipo de incidente é importante conhecer o contexto e as ações necessárias para uma mitigação desta ameaça. O Centro Nacional de Cibersegurança (CNCS) chama a atenção para as seguintes metodologias de ataque e boas práticas de prevenção.



METODOLOGIAS DE ATAQUE MAIS FREQUENTES

Este tipo de ataque pode ocorrer de diversas formas, contudo tende a seguir as seguintes fases:

RECONHECIMENTO

Os atacantes estudam previamente a organização-alvo de modo a identificar os colaboradores relevantes e as suas funções, os principais fornecedores assim como os principais contactos e domínios da organização. Podem recorrer para este efeito a informação em fontes abertas, como redes sociais profissionais ou a páginas Web institucionais, ou a dados expostos em fugas de informação.

PREPARAR O ACESSO INICIAL

Para iludir os colaboradores da organização-alvo, os atacantes comunicam através de mensagens de texto ou *emails* concebidos para serem facilmente confundidos com comunicações legítimas. Para o efeito, tendem a recorrer às seguintes técnicas:

- **Recurso a conta comprometida**: Nestes casos o atacante consegue garantir o acesso a uma conta de *email* conhecida, tipicamente de um fornecedor, colaborador ou de um superior hierárquico. Este acesso muitas vezes é obtido através da aquisição de credenciais em fóruns de cibercrime[1].
- **Recurso ao *spoofing***: Os atacantes falsificam frequentemente o remetente dos *emails* ou SMS através de uma técnica conhecida como *spoofing*. Esta técnica explora fragilidades na configuração dos domínios de *email* ou nas infraestruturas de telecomunicações para simular a identidade da organização-alvo, sem que tenha existido qualquer comprometimento das contas desta.
- **Recurso a domínios semelhantes aos da organização-alvo (*typosquatting*)**: O *typosquating* é frequentemente observado neste tipo de ataques e refere-se ao ato deliberado de registar um nome de domínio que explora variações tipográficas de um outro domínio-alvo já registado, em particular erros tipográficos frequentes na inserção do URL no *browser*.

[1] https://cncs.gov.pt/pt/contexto-atual-infostealers/.

Técnicas mais frequentes de *typosquatting*

a) **"*Missing-dot*"**: "https[://]wwwexemplo[.]pt"
b) **Omissão de caracter**: "www[.]exmplo[.]pt"
c) **Permutação de caracter**: "www[.]exemlpo[.]pt"
d) **Duplicação de caracter**: "www[.]exempllo[.]pt"
e) **Manipulação de TLD**: "www[.]exemplo[.]xyz"
f) **Manipulação de *punycode****: "xn--eemplo-bfg[.]pt" que no *browser* passa a "exemplo[.]pt"

*Sistema que permite a representação de caracteres não ASCII

ENGENHARIA SOCIAL

À semelhança de outros ataques de engenharia social, estes ataques exploram o fator humano, recorrendo a apelos à autoridade e à urgência, à confiança existente entre colaboradores assim como à pressão inerente às relações hierárquicas.
Partindo de contas ou contactos comprometidos, ou fazendo-se passar por entidades ligadas à organização-alvo, o atacante solicita a alteração de dados bancários associados a pagamentos correntes, de modo a desviá-los para contas sob o seu controlo. Estas comunicações assumem tipicamente uma das seguintes formas:

- **Pedidos de transferências bancárias urgentes**, alegadamente em nome do diretor(a) executivo(a) da organização-alvo;
- Envio de **faturas falsificadas** em nome de **fornecedores**, ou **pedidos de alteração de dados bancários** de um fornecedor com vista ao pagamento de faturas pendentes;
- Pedidos dirigidos ao **departamento de recursos humanos** para **alteração dos dados bancários de um colaborador**, com o objetivo de desviar o respetivo vencimento;
- A nível internacional, tem sido identificado o **recurso a *deep fakes***[2] para simularem superiores hierárquicos a pedirem ou autorizarem transferências ou pagamentos pouco comuns.

[2] Manipulação de vídeo ou voz com recurso a modelos de inteligência artificial generativa.

RECOMENDAÇÕES PARA EMPRESAS, ORGANISMOS DA ADMINISTRAÇÃO PÚBLICA E CIDADÃOS

a. Limitar, sempre que possível, a **visibilidade pública** de organigramas e contactos internos da organização, e sensibilizar os colaboradores para os riscos de publicarem informação profissional *online*, de modo a dificultar a recolha da informação necessária para este tipo de ataque.

b. Aplicar o **múltiplo fator de autenticação** em todas as contas da organização para evitar comprometimento de contas da organização;

c. Implementar mecanismos que garantam a autenticação nas comunicações por *email*, nomeadamente **SPF**, **DKIM** e **DMARC**.

d. Limitar a entrada de *emails* provenientes de **domínios registados recentemente** ou de domínios com pequenas variações tipográficas em relação aos da organização.

e. Implementar **sistema de gestão de fornecedores** que mantenha uma lista atualizada de fornecedores com pontos de contacto verificados, incluindo **pelo menos duas vias alternativas de contacto** para cada fornecedor.

f. Implementar medidas que garantam que **qualquer alteração de dados de fornecedor só pode ser realizada por este**. Por exemplo, no que respeita à mudança de IBANs, definir processualmente um período mínimo durante o qual a alteração não é aplicada, nem utilizada para pagamentos, até ser confirmada diretamente junto do fornecedor ou entidade (***hold out period*** [3]).

g. Sensibilizar os colaboradores das organizações para os seguintes cuidados:

> **a.** Verificar o endereço do remetente de *emails* recebidos ou o número de telemóvel de mensagens de texto, sobretudo se for solicitada informação sensível ou forem feitos pedidos críticos, como transferências bancárias;
>
> **b.** Sempre que é solicitada informação sensível ou feitos pedidos críticos por *email* ou mensagem de texto, confirmar com a entidade legítima, através de outro canal, se efetivamente fez alguma dessas ações;
>
> **c.** Confirmar pedidos de alteração de dados bancários com a própria entidade anunciada através de número de telefone conhecido e não do número inscrito na assinatura do *email* recebido, antes de ser promovida a alteração solicitada nos sistemas em uso;

[3] Período de segurança, com duração mínima predefinida, durante o qual uma alteração aos dados bancários fica suspensa e não produz efeitos em pagamentos, até ser confirmada diretamente junto da entidade visada.

d. Confirmar, no momento da transferência, o titular da conta bancária para a qual se pretende realizar uma transferência bancária em resultado de pedido por *email* ou mensagem de texto;

e. Verificar a linguagem e o estilo de comunicação ("tom") dos conteúdos dos *emails* e das mensagens de texto recebidos – muitas vezes esta linguagem não é coerente com o idioma utilizado em comunicações anteriores ou é descontextualizada. Pequenas diferenças de linguagem podem ser um indicador de fraude;

f. Suspeitar de *emails* ou mensagens de texto enviadas fora dos históricos das comunicações, principalmente se envolverem pedidos urgentes ou se solicitarem informação sensível ou ações críticas.

h. Realizar acordos com as entidades bancárias de modo a **criar mecanismos de verificação extra** na realização de transferências bancárias para minimizar possíveis consequências de um ataque deste tipo.

i. Assegurar a **segregação de funções na realização de operações bancárias**, recomendando-se que, sempre que possível, não seja um mesmo colaborador a iniciar e aprovar o pagamento sozinho.

j. Considerando o recurso a *deep fakes* em ataques ao nível internacional, recomenda-se atenção redobrada para este tipo de casos – **não confiar numa mensagem apenas porque usa imagem ou voz** que parecem reais.

CASO SEJA VÍTIMA

Caso seja vítima de um ataque deste tipo, **aconselha-se que sejam contactados o CERT.PT**, equipa de resposta a incidentes do CNCS (cert@cert.pt) e a **Polícia Judiciária** (unc3t@pj.pt).

TUTORIAL
COMO REPORTAR INCIDENTE

O CNCS DISPONIBILIZA

BOAS PRÁTICAS — CONSULTAR

CURSOS *ONLINE* GRATUITOS — CONSULTAR

RECURSOS DE SENSIBILIZAÇÃO, APRESENTAÇÕES PARA AS ORGANIZAÇÕES — CONSULTAR

A **CIBERSEGURANÇA** É UMA **RESPONSABILIDADE PARTILHADA.**

CENTRO NACIONAL DE CIBERSEGURANÇA
Rua da Junqueira, 69 | 1300-342 Lisboa
E-mail: cncs@cncs.gov.pt- Telefone: (+351) 210 497 400