CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

NOTA DE IMPRENSA

Contexto Atual CNCS

Campanhas de CEO Fraud e de Business Email Compromise Fraud (BEC)

Lisboa, 21 de abril, 2026 – O Centro Nacional de Cibersegurança (CNCS) alerta para um número crescente de casos de *CEO Fraud* e de *Business Email Compromise Fraud* (BEC), um tipo de incidente que tem afetado cidadãos e organizações e que pode resultar em perdas financeiras significativas.

As campanhas de *CEO Fraud/BEC*, que em 2025, correspondem a 18% dos incidentes de engenharia social notificados ao CERT.PT, 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.

Para uma organização se proteger deste tipo de ameaça é importante conhecer o contexto e as ações necessárias para a sua mitigação. O CNCS chama a atenção para as **metodologias utilizadas pelos atacantes e as boas práticas de prevenção disponíveis *online* no *site* institucional**. Destacam-se algumas:

- 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;
- Aplicar a autenticação multifator em todas as contas da organização para evitar comprometimento de contas da organização;
- Implementar mecanismos que garantam a autenticação nas comunicações por email, nomeadamente SPF, DKIM e DMARC;
- Limitar a entrada de emails provenientes de domínios registados recentemente ou de domínios com pequenas variações tipográficas em relação aos da organização;
- 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;
- Implementar medidas que garantam que qualquer alteração de dados de fornecedor só pode ser realizada por este.

Com o novo Regime Jurídico da Cibersegurança, o CNCS reforça o seu papel central na proteção do ciberespaço nacional, no apoio às entidades públicas e privadas e na promoção da literacia digital dos cidadãos, com vista à promoção de uma cultura de cibersegurança e de um ecossistema +Resiliente. Neste sentido, sempre que necessário, o CNCS, informa sobre situações, circunstâncias extraordinárias, ameaças relevantes e recomendações, que exijam especial atenção.

Rua da Junqueira, 69, 1300-342, Lisboa • Tel (+351) 210 497 400 • cncs@cncs.gov.pt

Mais informações: https://www.cncs.gov.pt/pt/contexto-atual-ceo-fraud/
Boas práticas: https://www.cncs.gov.pt/docs/ceofraud_boas_praticas.pdf
Recurso de sensibilização para organizações: https://www.cncs.gov.pt/docs/ceofraudbec.pdf