https://www.cncs.gov.pt/pt/boas-praticas-contra-o-phishing-o-smishing-e-o-vishing/

BOAS PRÁTICAS CONTRA O PHISHING, O SMISHING E O VISHING

O QUE SÃO

O *phishing* é um tipo de ataque em que se usam técnicas de engenharia social para capturar informação sensível de uma vítima através de *email.* Um agente de ameaça que utilize este tipo de ataque procura enganar os recetores de *emails* para que estes disponibilizem informação sensível através do clique em anexos e/ou URL maliciosos ou da partilha de dados em páginas fraudulentas. Para o efeito, o atacante simula uma marca credível ou personifica alguém de confiança. Quando esta técnica é utilizada através de SMS, dá pelo nome de *smishing* e, por telefone (voz), de *vishing*. Esta técnica também pode ser usada através de mensagens instantâneas em aplicações de redes sociais.

O que fazer

- Não clicar em anexos ou *links* de *emails,* de mensagens instantâneas ou de SMS suspeitos;
- Quando se é contactado, confirmar a veracidade do endereço de *email*, do perfil ou do número de telefone de origem;
- Avaliar sempre a oportunidade dos conteúdos de *emails,* de mensagens instantâneas, de SMS ou de telefonemas;
- Não partilhar dados pessoais ou seguir instruções sem verificar noutras fontes a veracidade do pedido – por exemplo, junto do gestor de conta do Banco ou de um superior hierárquico;
- Desconfiar de mensagens com erros formais de linguagem, mas também não confiar em todas as mensagens apenas porque não apresentam erros formais de linguagem;
- Nas organizações, realizar simulações de ataques de *phishing* e *smishing,* e eventualmente de *vishing,* de modo a aumentar a sensibilização e os níveis de atenção a estes meios;
- Não partilhar dados sensíveis nas redes sociais porque essa prática pode fornecer informação a possíveis atacantes que queiram realizar *spear phishing* (*phishing* dirigido a uma pessoa específica);
- Denunciar junto dos responsáveis de segurança informática da organização ou junto das autoridades sempre que se é alvo ou vítima de um ataque deste tipo;
- Estar atento e não se deixar persuadir sem reflexão por solicitações autoritárias, promessas ou pedidos urgentes.

Dados

- O *phishing* e o *smishing* têm sido os tipos de incidentes mais registado pelo CERT.PT: em 2019 corresponderam a 31% dos incidentes registados e em 2020 a 43%, tendo subido, nesse ano, em termos absolutos, 160% (CNCS, Riscos e Conflitos 2021);
- Verifica-se que 2021 manteve uma trajetória ascendente e que os períodos com maior volume de incidentes, em particular de *phishing* e *smishing,* foram os de maior confinamento social fruto da pandemia da Covid-19 (CNCS, Boletim n.º 4/2021);
- Segundo uma análise de conteúdo feita ao *phishing* e ao *smishing* registados pelo CERT.PT durante o segundo trimestre de 2020, verifica-se que o tipo de persuasão mais utilizado pelos atacantes, em 90% dos casos, é o argumento da autoridade/credibilidade do emissor (um Banco, por exemplo), 79% das mensagens incentivam o *login* numa conta, 12% pedem dados relacionados a um produto/serviço, 7% prometem um ganho financeiro e 3% referem-se ao preenchimento de um documento (CNCS, Boletim n.º 3/2020).

Acedido em 17-05-2022