PROTEJA-SE CONTRA

FRAUDES DIGITAIS

INFORMAÇÃO ESSENCIAL PARA O CONSUMIDOR

PROTEJA-SE CONTRA
FRAUDES DIGITAIS

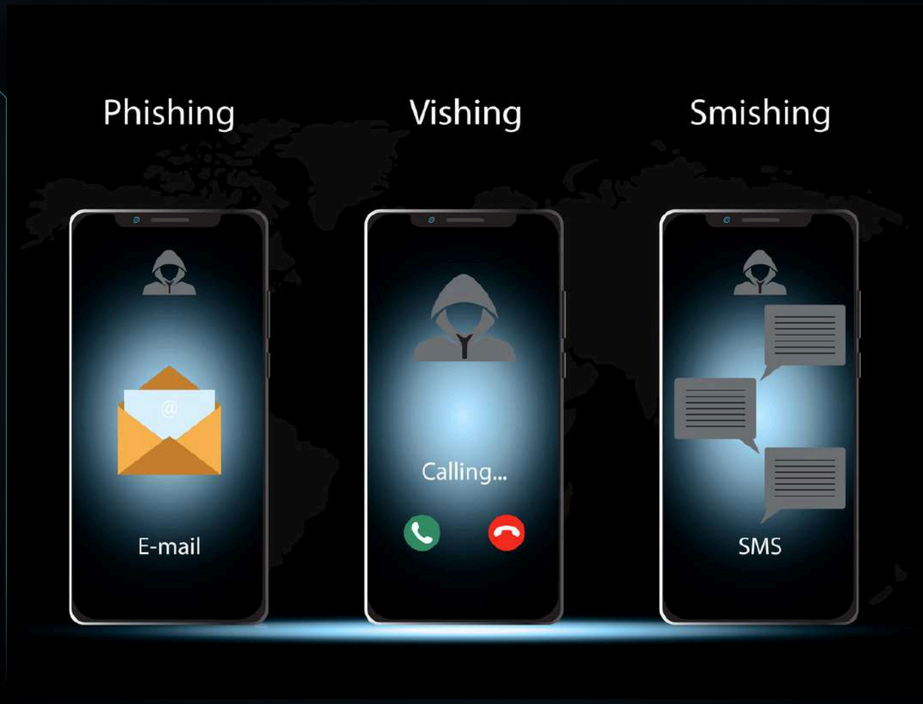
No atual contexto digital, o aumento das interações *online* trouxe consigo novos riscos, nomeadamente, nas formas como criminosos cibernéticos procuram explorar a confiança e a distração dos utilizadores para cometer fraudes.

É fundamental que todos estejam informados e preparados para proteger os seus dados pessoais e financeiros contra estas ameaças crescentes.

O QUE SÃO FRAUDES DIGITAIS?

Fraudes digitais são esquemas ilegítimos realizados através da internet, telefone ou outras plataformas digitais, com o objetivo de obter informações pessoais, credenciais bancárias ou induzir a vítima a realizar pagamentos sob falsas justificações.

Entre as formas mais comuns de fraude digital em Portugal encontram-se o *Vishing, o Typosquatting, o Phishing e o Pharming*.



VISHING

O *vishing*, combinação das palavras em inglês *voice* (voz) e *phishing* (burla digital), é uma forma de fraude que ocorre através de chamadas telefónicas.

Os perpetradores destas ações fingem ser entidades de confiança, como bancos, empresas ou autoridades, e tentam convencer a vítima a divulgar dados pessoais ou bancários, muitas vezes criando um sentimento de urgência ou emergência.

TYPOSQUATTING

Também conhecido como *“ciberocupação por erro tipográfico”*, o *typosquatting* consiste no registo de domínios web com nomes muito semelhantes aos de marcas legítimas, aproveitando pequenos erros comuns de digitação para enganar os utilizadores.

Estes sites falsos são concebidos para parecer autênticos e recolher dados pessoais, instalar software malicioso ou direcionar para esquemas fraudulentos.

PHISHING

Phishing é uma fraude que normalmente ocorre quando criminosos se fazem passar, através de e-mails fraudulentos, por instituições legítimas para roubar informações confidenciais.

Existem várias formas, incluindo ataques personalizados (*spear phishing)*, mensagens SMS fraudulentas *(smishing)*, entre outras.

SPEAR PHISHING

É uma forma de *phishing* direcionada a uma pessoa ou organização específica, onde o atacante adapta a mensagem para parecer legítima e relevante para a vítima, aumentando as hipóteses de sucesso.

Este tipo de ataque é muitas vezes utilizado para obter acesso a informações sensíveis ou sistemas corporativos.

SMISHING

Envolve o envio de mensagens SMS fraudulentas que contêm *links* maliciosos ou pedidos de informações pessoais.

As vítimas são induzidas a clicar em *links* que podem instalar *malware* no dispositivo ou redirecionar para sites falsos que capturam dados confidenciais.

Outras formas incluem o clone *phishing*, onde *emails* legítimos previamente enviados são copiados e enviados com links ou anexos maliciosos.

Estes ataques exploram a confiança natural das vítimas, frequentemente criando um sentido de urgência, medo ou distração para as levar a agir sem a devida cautela.

A **manipulação psicológica** é um dos principais mecanismos utilizados, induzindo as vítimas a fornecer informações pessoais, senhas, dados financeiros ou até mesmo a permitir o acesso a sistemas informáticos corporativos.

Além disso, estes métodos aproveitam falhas humanas mais do que tecnológicas, o que torna a educação e a sensibilização dos utilizadores ferramentas fundamentais para a prevenção.

Estar atento aos detalhes das mensagens, verificar a veracidade das fontes e adotar práticas seguras, como a autenticação multifatorial e a alteração regular de passwords, são medidas essenciais para reduzir a exposição a estas fraudes.

Nunca deve fornecer informações sensíveis sem confirmação adequada, e em caso de qualquer suspeita, deve-se procurar imediatamente aconselhamento junto dos serviços de apoio ao consumidor ou das autoridades especializadas em segurança da informação.

PHARMING

O *pharming* redireciona o utilizador para sites falsos, mesmo que ele insira o endereço correto, através da manipulação técnica de sistemas de DNS ou do navegador.

É uma ameaça que compromete a segurança ao nível do sistema.

COMO IDENTIFICAR E PROTEGER

Nunca forneça dados pessoais ou bancários por telefone, email ou mensagens, mesmo que pareçam ser de entidades oficiais:

· Confirme a autenticidade de chamadas ou comunicações contactando diretamente as entidades por canais oficiais.

· Esteja atento a pedidos urgentes ou que criem pressão para decisões rápidas.

· Utilize autenticação de dois fatores nas suas contas online para maior segurança.

· Mantenha os seus dispositivos e programas de segurança sempre atualizados.

· Verifique cuidadosamente o endereço dos sites que visita e evite clicar em links suspeitos.

EM CASO DE SUSPEITA DE FRAUDE:

· Não forneça informações adicionais.

· Feche o navegador e altere as suas palavras-passe.

· Guarde todas as evidências do incidente.

· Denuncie imediatamente às autoridades de proteção e segurança digital.

A INFORMAÇÃO É A MELHOR DEFESA

A CONSCIENCIALIZAÇÃO E A PRECAUÇÃO SÃO ESSENCIAIS PARA EVITAR FRAUDES DIGITAIS.

ESTAR INFORMADO, AGIR COM CAUTELA E MANTER-SE ATUALIZADO CONTRIBUI PARA A SUA PROTEÇÃO E A SEGURANÇA DOS SEUS DADOS NA ERA DIGITAL.