CRÓNICA DO OBEGEF
Nº 104 /2024-11-21
http://www.obegef.pt

Raquel Brito

> > Fraude eletrónica – Tipologias e medidas preventivas

No mundo contemporâneo o incessante desenvolvimento tecnológico chega já a inúmeras e longínquas áreas geográficas. Acompanhado de um crescimento exponencial, este desenvolvimento, torna (quase) inevitável o uso generalizado de diversos equipamentos eletrónicos (computadores, smartphones, tablets, entre outros) expondo os seus utilizadores a riscos inerentes ao ciberespaço. A fraude eletrónica, um destes riscos, reveste-se de atividades fraudulentas que ocorrem através de meios eletrónicos, geralmente na internet. Este tipo de fraude pode envolver uma diversidade de práticas ilícitas, e é frequentemente direcionado a indivíduos, empresas ou instituições financeiras.

A fraude eletrónica, cada vez mais complexa e sofisticada, apresenta atualmente uma panóplia considerável de tipologias, particularmente: ***Phishing*** - Tentativas de obter informações pessoais, como *passwords* e/ou dados bancários, utilizando e-mails falsos ou websites que procuram substituir-se a instituições legítimas; ***Smishing*** e ***Vishing*** - Variedades de *phishing* que ocorrem via mensagens (*smishing*) ou chamadas telefónicas (*vishing*), onde os defraudadores tentam enganar as vítimas de forma a que partilhem informações sensíveis; **Clonagem de cartões de crédito** - Roubo de informações de cartão de crédito através de *malware*, *skimmers* ou compra de dados em mercados clandestinos; **Roubo de Identidade** - Uso das informações pessoais de alguém sem o seu consentimento para cometer fraudes, como abrir contas bancárias ou solicitar empréstimos; **Fraude em compras *Online*** - Vendas fraudulentas em plataformas de e-commerce, onde produtos que não existem ou são de qualidade inferior são oferecidos; ***Malware*** e ***Ransomware*** - Programas maliciosos que podem roubar dados, usurpar

informações ou exigir pagamento para a liberação de dados; ***Fraude em Investimentos*** - Promessas de elevados retornos em investimentos que são, na verdade, esquemas *Ponzi* ou fraudes de investimento.

Mergulhados neste contexto tecnológico, somos diariamente contemplados com inúmeras interpelações que nos poderão conduzir a pertencer a este grupo de lesados, e cujas mensagens podem assumir as mais diversas formas e apresentar os mais distintos conteúdos. Quem, em boa verdade, nunca se viu confrontado com mensagens que, não tendo gerado desconfiança, geraram um certo desconforto?

São alguns exemplos:

> *"Olá mãe, Olá Pai…";*
>
> *"Olá Pedro, neste momento estou de férias em Angola e preciso trocar euros por kwanzas…";*
>
> "*Identificamos divergências (IRS) – Notificação 7295770930"* (https://info.portaldasfinancas.gov.pt/pt/destaques/Paginas/AvisoSeguranca.aspx);
>
> *"Prezado cliente, a sua fatura esta pendente. Pague até 14/11 para evitar suspensão. MB: Entidade...Referência…Valor…"*

Estas mensagens fraudulentas apresentam-se em grupos principais, nomeadamente: a) mensagens que personificam uma pessoa conhecida ou uma organização com vista a conduzir a vítima a realizar transferências bancárias para um agente malicioso; b) Mensagens que personificam uma organização com o objetivo de recolher informação sensível, como palavras-passe ou números de cartões de crédito; e c) Mensagens que procuram conduzir o utilizador a instalar programas maliciosos que comprometem a segurança do dispositivo (https://www.cncs.gov.pt/pt/boas-praticas-contra-mensagens-instantaneas-fraudulentas/).

De acordo com o Centro Nacional de Cibersegurança (CNCS) *"É através destas mensagens que muitas fraudes ocorrem, afetando qualquer tipo de pessoa que tenha um*

smartphone, mesmo que não use um computador." Este serviço de envio de mensagens instantâneas (uma das funcionalidades mais utilizada nos smartphones) é desenvolvido por aplicações especificas ou através de redes sociais. Este mesmo organismo divulga ainda dados resultantes de um inquérito europeu realizado em 2021 que revelam que em Portugal *"…91% dos inquiridos afirmaram utilizar aplicações de mensagens instantâneas, mais 12 pp do que a média da União Europeia."*.

No campo da prevenção existe atualmente uma elevada preocupação, por parte das instituições competentes, na divulgação de medidas preventivas, nomeadamente:

1. Educação e conscientização sobre estas matérias, procurando familiarizar os utilizadores com os tipos de fraudes eletrónicas, tornando-os vigilantes a e-mails e mensagens suspeitas. Alegações de urgência ou de oportunidade única devem gerar suspeitas bem como a existência de erros ortográficos.
2. Verificação da fonte: Verificar sempre se o remetente de um e-mail ou mensagem é legítimo antes de partilhar informações pessoais ou aceder a links.
3. Definir senhas fortes: Escolher senhas complexas e únicas para diferentes contas alterando-as periodicamente.
4. Manter o *software* atualizado: Garantir que o sistema operacional, aplicativos e *software* de segurança estão sempre atualizados para proteção de qualquer vulnerabilidade.
5. Cuidados redobrados com *Wi-Fi* público: Evitar transações financeiras e/ou acessos a dados sensíveis em redes Wi-Fi públicas, que podem ser facilmente intercetadas.
6. Monitorização de contas bancárias: Regularmente verificar extratos bancários e de cartão de crédito para detetar transações não autorizadas.
7. Utilização de *software* de segurança: Usar antivírus e *firewalls* para proteger dispositivos contra *malware* e outras ameaças.

A denúncia às autoridades competentes inclui-se nos contributos de prevenção e combate a esta criminalidade. Neste quadro, foi divulgada recentemente pela Polícia Judiciária (PJ detém suspeito de burla "Olá mãe, Olá pai" – Polícia Judiciária a detenção um individuo indiciado pela prática dos crimes de associação criminosa, branqueamento e burla qualificada vulgarmente conhecida como "Olá mãe, Olá pai", um dos casos de fraude eletrónica mais denunciados ao Gabinete Cibercrime do Ministério Público no ano de 2022 (CNCS).

Em suma, prevenir a fraude eletrónica requer atenção contínua e medidas de segurança, mas com o conhecimento adequado e a implementação de práticas seguras, é possível minimizar os riscos. Quer a prevenção quer o combate revelam-se árduas tarefas por diversos fatores, mas essencialmente pelo imparável avanço tecnológico que proporciona um ambiente favorável à igualmente imparável imaginação humana.