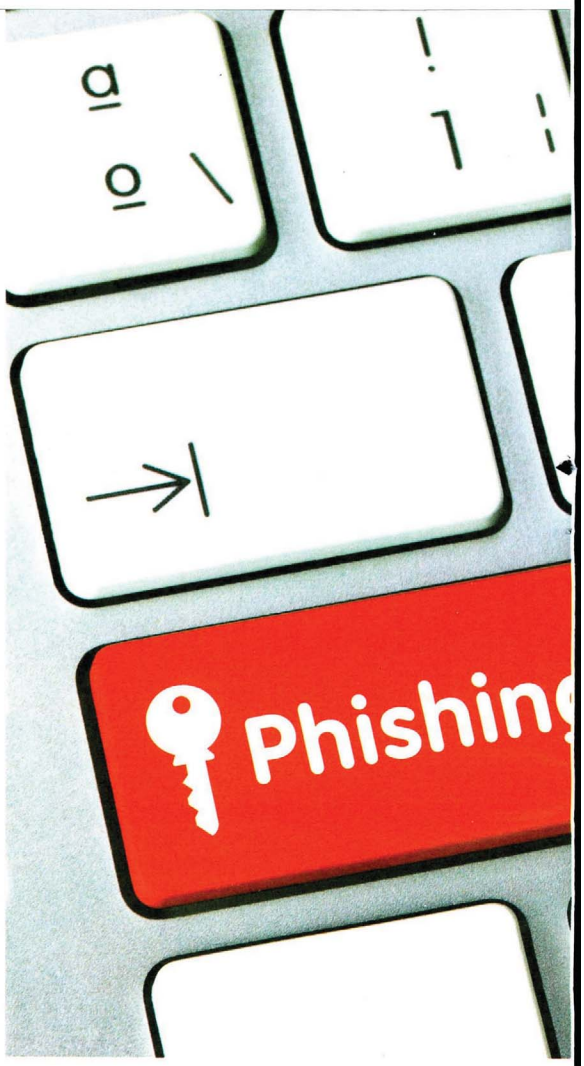
CISION

ID: 111918076

02-07-2024

Meio: Imprensa
País: Portugal
Área: 11306,82cm²
Âmbito: Informação Geral
Period.: Semanal
Pág: 2-19,1

Burlas online. Phishing é o crime mais denunciado



As fraudes mais comuns envolvem a compra e venda de bens e, surpreendentemente, as burlas via MB Way diminuíram entre 2022 e 2023. No entanto, os jovens têm uma maior probabilidade de serem enganados.

MARIA MOREIRA RATO
maria.rato@ionline.pt

Quando pensamos em burlas online, lembramo-nos, muitas das vezes, da famosa "burla do príncipe da Nigéria", que é uma forma de fraude conhecida como "esquema de adiantamento de fundos" ou "fraude 419" (em referência ao artigo do Código Penal nigeriano que aborda fraudes). Este golpe tem várias variações, mas, habitualmente, tudo tem início quando a vítima recebe um e-mail ou uma mensagem de alguém que alega ser um príncipe nigeriano, um funcionário do Governo ou uma pessoa rica em dificuldades. A partir daí, tudo se desenrola e, em troca da ajuda da vítima, o burlão promete uma generosa recompensa, frequentemente uma percentagem significativa da quantia total de uma fortuna que alegadamente está inacessível devido a complicações legais ou políticas.

Contudo, as burlas são cada vez mais sofisticadas e têm vindo aumentar nos últimos anos e Portugal não é uma exceção à regra. Em março, a Guarda Nacional Republicana (GNR) alertou para o aumento das burlas online. De acordo com os dados divulgados, houve um aumento de 3.579 casos de 2022 para 2023 em todo o país. Em 2022, a GNR registou 17.969 crimes de fraude, com destaque para as fraudes informáticas e de comunicações, que totalizaram 6.518 ocorrências, e fraudes bancárias, com 2.630 registos. Em 2023, os números subiram para 21.548 crimes de fraude, incluindo 7.303 fraudes informáticas e de comunicações e 3.079 fraudes bancárias.

Os distritos mais afetados foram Porto, Setúbal e Lisboa, embora existam dados apurados em todo o país. A GNR destaca que as fraudes mais comuns envolvem a compra e venda de bens, o MB Way e publicações na internet. As fraudes com MB Way foram as únicas a apresentar uma diminuição entre 2022 e 2023.

"É difícil dizer quais são os principais tipos de burla online porque são cada vez mais variadas. Em termos genéricos, o *phishing* será o mais denunciado. Nestes casos, o principal objetivo dos atacantes tem sido aceder a dados de cartões bancários, mas também a plataformas de *homebanking* (embora neste caso se exija maior sofisticação, devido aos mecanismos de segurança implementados)", começa por explicar ao *i* David Silva Ramalho, associado coordenador da Morais Leitão, Galvão Teles, Soares da Silva & Associados, que integra a equipa de criminal, contraordenacional e compliance da Sociedade.

'OLÁ MÃE, OLÁ PAI' "No entanto, dentro desta categoria existem várias modalidades e vários modos de execução (por *chats*, por *WhatsApp*, por *Telegram*, por email, etc.). Noutra vertente, temos também visto um aumento das burlas 'Olá mãe, olá pai', os contactos a pedirem pagamento de falsas dívidas à Autoridade Tributária, a bancos ou a prestadores de serviços, os contactos falsos provenientes da polícia a exigir pagamentos, os falsos arrendamentos, as burlas em mercados online, entre muitas outras", avança o advogado.

"Além destas, tenho lidado muito, desde logo porque também me tenho especializado nesta área, com burlas com criptomoedas, em que os atacantes, implementando verdadeiros mecanismos de apoio ao cliente, criam falsas plataformas online, com áreas reservadas, que as vítimas podem consultar e onde são levadas a crer que estão a ver os seus investimentos a crescer", afirma, adiantando que "para eliminar o rasto, dos pagamentos, é frequente os atacantes levarem as vítimas a criarem contas em seu próprio nome, em bancos estrangeiros, levando-as a facultar as credenciais e a gestão efetiva da conta a esses mesmos atacantes". "Depois, quando se procura obter informação sobre o titular da conta, só se obtêm dados da vítima", alerta.

"A vítima de burla tem sempre o direito a ser ressarcida, pelo menos por parte do atacante. O problema aqui não está nos direitos da vítima, mas sim na dificuldade em exercê-los, já que grande parte desses direitos passa pela identificação do autor do crime, o que é difícil por natureza no cibercrime, mas especialmente considerando a escassez de meios da investigação criminal", diz o também investigador no Centro de Investigação em Direito Penal e Ciências Criminais (CIPDCC) e associado do Instituto de Direito Penal e Ciências Criminais (IDPCC). "A lei prevê também, em certos casos, a possibilidade de a vítima obter o reembolso por parte do prestador do serviço de pagamento, desde que verificados os requisitos legais".

"É preciso denunciar estes crimes, mesmo que se ache que não se vai recuperar os valores"

David Silva Ramalho
ADVOGADO DA MORAIS LEITÃO

Por falar nas vítimas, as mesmas têm recorrido igualmente ao Portal da Queixa para revelarem os crimes de que são alvo naquilo que diz respeito, principalmente, às compras online. Por exemplo, entre janeiro e março deste ano, os consumidores em Portugal registaram 1.313 queixas sobre fraudes online, um aumento de aproximadamente 20% em relação ao mesmo período de 2023. De acordo com o Portal da Queixa, até 21 de abril, o número de reclamações já havia alcançado 1.486. A maioria das queixas refere-se a compras realizadas em lojas virtuais, onde os consumidores alegam não receber os produtos adquiridos, ficando sem resposta dos vendedores e sem o reembolso do valor pago.

COMPRAR E FICAR A VER NAVIOS

O motivo principal das reclamações é a ausência de reembolso após a não entrega do produto, representando 57,8% dos casos de fraude. Outro problema apontado é a dificuldade de comunicação com a marca, incluindo atendimento ao cliente ineficaz e falta de retorno dos vendedores. A maior parte das queixas de fraudes, representando 42,5% das denúncias, está na categoria de Compras, Moda e Joalharia. A seguir, a categoria de Beleza, Estética e Bem-Estar reúne 13,6% das queixas. Além disso, 9,4% das reclamações são sobre fraudes em Hotéis, Viagens e Turismo, enquanto 9% estão relacionadas com lojas de Mobiliário, Decoração e Eletrodomésticos. Lojas online, Sites e Negócios são responsáveis por 7,4% das queixas. No ano passado, o Portal da Queixa recebeu aproximadamente 25 mil reclamações sobre fraudes online, um

CISION

ID: 111918076

02-07-2024

Meio: Imprensa
País: Portugal
Área: 11306,82cm²
Âmbito: Informação Geral
Period.: Semanal
Pág: 2-19,1

Os portugueses têm de ter mais atenção às mensagens enganosas que parecem ser de fontes confiáveis, mas estão mais conscientes dos perigos do MB Way

FOTOS: DR

aumento de 37% em relação ao mesmo período de 2022.

"A vítima de burla deve imediatamente contactar o seu banco e tentar cancelar a transferência ou pelo menos pedir a comunicação ao banco de destino de que se trata de uma transferência fraudulenta. Neste ponto, é importante referir que existem bancos que, se a vítima não tiver *homebanking*, apenas aceitam esta comunicação ao balcão, o que leva a que, nas burlas ocorridas à sexta-feira (e são muitas), não se consiga fazer nada até às manhãs de segunda", explica. "Além do contacto com o banco, a vítima deve dirigir-se à Polícia Judiciária e apresentar uma denúncia, preferencialmente acompanhada de advogado. No caso das burlas de criptomoedas, para facilitar a investigação, o ideal é que seja o próprio advogado a fazer o tracing das criptomoedas, para facilitar a investigação criminal".

Quanto às medidas tomadas em relação aos denominados burlões, afirma que "primeiro, as medidas preventivas, ainda que não legais: sempre que há uma mudança de dados de pagamento, deve-se confirmar por outros meios de comunicação se essa mudança é real; sempre que se recebe pedidos de pagamento de instituições com quem se tem ou não se tem contratos, é preciso confirmar a sua veracidade, se necessário contactando as próprias, e, por fim, é preciso desconfiar de promessas de lucros elevados em curtos espaços de tempo", frisa. "Por outro lado, é preciso denunciar estes crimes, mesmo que se ache que não se vai recuperar os valores. Quando se chega aos burlões, haverá que recorrer ao processo-crime, procurando o imediato congelamento de bens e quaisquer outras medidas que garantam a sua responsabilização e o ressarcimento das dívidas".

> "A vítima de burla deve imediatamente contactar o seu banco"

Um estudo da Deloitte chegou à conclusão de que os jovens caem mais facilmente em burlas

Quanto ao papel das autoridades nestas situações, realça que estas "têm a difícil tarefa de investigar todos estes crimes, sem meios para o efeito, e com uma legislação que, no plano processual, podia e devia ser atualizada", sendo que "o primeiro passo é tentar identificar os burlões, o que se revela quase sempre de grande dificuldade, especialmente quando estão no estrangeiro. Pelo meio, e independentemente de se encontrar o suspeito, é necessário ir atrás dos bens, identificar as mulas que recebem os valores para depois os transferirem para os atacantes e tentar desmontar a organização, quando exista", declara David Silva Ramalho. "O problema é que os crimes informáticos são genericamente da competência da Polícia Judiciária, que tem de investigar, com recursos escassos, as burlas de milhões, as burlas de milhares, as de centenas e as de dezenas de euros, o que implica ter de gerir vários processos, promover várias diligências junto das autoridades judiciárias, inquirir várias testemunhas, e concluir várias investigações, sem que seja possível fazê-lo no tempo desejável", explicita.

"A primeira parte, e geralmente a mais difícil, é encontrar os suspeitos. É necessário fazer várias diligências, como seja identificar o IP e os dados de subscrição a ele associados, pedir informações a instituição de pagamento, emitir Decisões Europeias de Investigação ou cartas rogatórias, e, muitas vezes, é necessário que o atacante cometa erros, para se chegar a uma ou mais pessoas concretas", continua. "Este período pode demorar meses ou anos, dependendo da complexidade do crime, do rasto que se encontre, da dimensão nacional ou internacional ou do carácter mais ou menos organizado do crime. Uma vez identificado o suspeito e deduzida acusação, o processo corre os seus termos com a celeridade habitual nos nossos tribunais, podendo estar concluído num prazo não muito longo", conclui o advogado.

JOVENS DA GERAÇÃO Z CAEM MAIS EM BURLAS ONLINE Embora os jovens e tecnicamente experientes possam estar à vontade na internet, a Geração Z – nascida entre 1995 e 2012 – tem três vezes mais probabilidade de ser vítima de fraudes online quando comparada com os baby boomers, segundo um relatório de 2023 da Deloitte. Comparadas com as gerações mais velhas, as mais jovens relataram taxas mais altas de vitimização em *phishing*, roubo de identidade, fraudes românticas e *cyberbullying*. A pesquisa da Deloitte revela que os norte-americanos da geração Z têm três vezes mais probabilidade de serem vítimas de fraudes online do que os boomers, com 16% contra 5%, respetivamente.

Além disso, a Geração Z é duas vezes mais propensa a ter uma conta de rede social hackeada em comparação com os boomers, com 17% contra 8%. Catorze por cento dos entrevistados da Geração Z relataram que as suas informações de localização foram mal utilizadas, uma taxa maior do que qualquer outra geração. O custo de cair nesses golpes também parece estar aumentando para os mais jovens: o relatório de 2023 da Social Catfish sobre golpes online descobriu que vítimas de golpes online com menos de 20 anos perderam cerca de 8,2 milhões de dólares (aproximadamente 7.63 milhões de euros) em 2017, enquanto em 2022, as perdas chegaram a 210 milhões (cerca de 195 milhões de euros).