

**Radar**

Na maioria das vezes,
os burlões roubam dados
e conseguem extorquir
dinheiro via MBWay,
mas agora também
o fazem de outros modos

DR



Burlões com novas técnicas para enganar e extorquir dinheiro e dados

Há cada vez mais pessoas com medo de abrirem emails, SMS e até ligações em redes sociais. A PSP, a PJ e um especialista em cibercrime deixam conselhos para que se sintam mais seguros.

MARIA MOREIRA RATO
maria.rato@jonline.pt

As burlas têm vindo cada vez mais a serem otimizadas por aqueles que ganham dinheiro a enganar os outros. Principalmente, desde o início da pandemia de covid-19. No entanto, nos últimos tempos, são cada vez mais as pessoas que não se sentem seguras quando acedem às redes sociais, ao email ou simplesmente consultam as SMS.

É o caso de Joana (nome fictício), de 42 anos, cuja fotografia

do WhatsApp foi roubada por alguém, cuja identidade é desconhecida, que com outro número de telemóvel, contactou a sua irmã. "Tentou burlá-la, não deu, a seguir troca a foto de perfil e continua a enganar outra pessoa", desabafa, em declarações ao *i*. "Mas esse número tem de estar associado a uma conta de MBWay porque eles pedem dinheiro e a conta tem de ser de alguém", continua, lembrando que as mensagens enviadas à sua irmã foram posteriormente apagadas pelo burlão.



CIBERCRIME



Outras formas de obter dinheiro e dados passam por enviar mensagens semelhantes às que um banco poderia enviar. A título de exemplo: "Montepio: Cartão de Débito e PIN foram bloqueados. Para desbloquear "aceda a" seguido de um link "e confirme os seus dados", assim como emails em que o destinatário é incentivado à ação. Imaginemos: "Ana, tentámos entregar a sua encomenda dos CTT Expresso na morada indicada" com emojis e texto – habitualmente, repleto de erros ortográficos – que, claramente, jamais seriam enviados pelos verdadeiros correios de Portugal.

No entanto, os burlões não ficaram por aqui – nem pelo célebre "Olá, mãe! Olá, pai!" – e, por isso, decidiram fazer-se passar pelas autoridades. "Olá. Nossos agentes detetaram uma violação do seu dispositivo, esta ação é uma ofensa passível de ação legal. Por favor, leia o anexo com atenção e responda assim que recebê-lo, caso contrário uma intimação oficial será enviada a você dentro de 72 horas", lê-se no início de uma mensagem em que a "Diretora Geral da Gendarmaria Nacional" assina, jun-

tamente com o "Sr. Botelho Miguel" eleito para o cargo de "Comandante-Geral da GNR, Comissário Divisional, Chefe da Brigada para a Proteção de Menores (CPCJ)" um texto acusando aquela que poderá ser uma vítima de crimes como abuso sexual de menores, posse de pornografia infantil, exibicionismo, tráfico sexual, entre outros. Incluindo, para este efeito, de melindrar o destinatário, mais o nome, do "Sr. José Manuel dos Santos Pais, Procurador-Geral do Tribunal de Recurso de Paris e especializado em cibercrime".

Contactada pelo *i*, a Polícia de Segurança Pública (PSP) declara que "tem conhecimento da circulação do e-mail fraudulento em apreço tendo, inclusive, feito um alerta nas redes sociais no passado dia 18 de outubro", acrescentando que ajuda diretamente quem lhe faz chegar denúncias. "Sempre que temos conhecimento deste tipo de situações, além do alerta que fazemos através das N/ redes sociais, ainda enviamos um e-mail de resposta a todas as pessoas que nos fazem chegar este tipo de denúncias, com conselhos e medidas de segurança que podem

ser levadas a cabo por parte dos lesados", conclui a PSP.

Já a Polícia Judiciária (PJ) informa, também em declarações ao *i*, "que se trata de uma tentativa de burla e que, através da UNC3T, tem alertado para este tipo de situações", sendo que "disponibiliza várias informações e conselhos preventivos que se encontram na página oficial da PJ, através dos seus 'Alertas ao Cidadão' e nas suas redes sociais (Facebook, Instagram, Twitter e YouTube),

A PSP "tem conhecimento do e-mail fraudulento" e "fez um alerta nas redes sociais"

Um advogado especialista em cibercrime partilha dicas para que navegue em segurança

bem como algumas informações e campanhas de prevenção de parceiros internacionais com quem a PJ colabora, igualmente noticiadas e disponíveis através dos mesmos canais".

AS TRÊS CAMADAS DE PROTEÇÃO As pessoas "caem nestas armadilhas"? Infelizmente, "sim", começa por afirmar David Silva Ramalho, advogado e associado principal na equipa de Contencioso Criminal, Risco e Compliance da Moraes Leitão. "E a circunstância de o modo de execução das burlas ir mudando, leva a que os alertas acabem por se desatualizar depressa. A massificação do uso de tecnologias de informação, incluindo por camadas da população com menos literacia informática, e a tendência para se partilhar muita informação pessoal em redes sociais sem quaisquer restrições de acesso, torna-nos alvos fáceis deste tipo de tentativas", observa o assistente convidado na Faculdade de Direito da Universidade de Lisboa.

"Como para praticar estes crimes basta ter um telemóvel, um cartão pré-pago ou acesso à Internet, o risco para o agente é per-

cebido como sendo relativamente diminuto. A partir daí basta ao agente do crime iniciar uma campanha de tentativas, muitas vezes adaptada ao seu interlocutor com base em informação recolhida em fontes abertas, e alguém há-de cair".

"A primeira camada de proteção é prévia aos crimes. As pessoas têm de perceber que não podem partilhar tanta informação nas redes sociais sem qualquer restrição. A tentação de ter cada vez mais seguidores, de adicionar desconhecidos como amigos para trocar prendas em jogos online, de publicar fotografias da família, de celebrar aniversários nos murais, de marcar pessoas como familiares, expõe-nos a variadíssimos riscos, dos quais o phishing é apenas um", aconselha o investigador no Centro de Investigação em Direito Penal e Ciências Criminais (CIPDCC) e associado do Instituto de Direito Penal e Ciências Criminais (IDPCC).

"Uma segunda camada de proteção é partir sempre de um pressuposto de desconfiança quando alguém nos pede dados pessoais ou dinheiro. Se uma pessoa com quem temos intimidade suficiente para emprestar dinheiro muda de número e nos pede dinheiro por essa via, vale a pena telefonar-lhe ou confirmar que é de facto essa pessoa por qualquer outra via. Se o Banco nos envia um link por SMS e nos pede para introduzirmos as credenciais, vale a pena ver se o link é mesmo do Banco e se aquela é a página certa. O melhor é fechar a página e ir à do Banco", continua. "Se alguém nos pede credenciais bancárias por via remota, telefone ou internet, devemos evitar fazê-lo, e se quisermos fazê-lo, devemos confirmar antes se aquela pessoa é mesmo quem diz ser", recomenda o advogado e professor.

"Uma terceira camada de proteção é ter cuidado ao navegar na Internet. Ter cuidado com os sites que visitamos, ter cuidado ao instalar add-ons e aplicações, escolher palavras-passe diferentes para diferentes websites, não partilhar dados de pagamento (desejavelmente utilizar cartões descartáveis com plafonds máximos) e preocuparmo-nos com a nossa privacidade", recorda. "Há uma tendência generalizada para se dizer que não temos nada a esconder, não temos de nos preocupar com privacidade. Mas por algum motivo temos persianas nas janelas de casa. E por algum motivo trancamos a porta quando saímos".

INEVITÁVEL

PSP E GNR USADAS COMO ISCO DE BURLÕES DA INTERNET

São cada vez mais os esquemas inventados para enganar os incautos que respondem a emails, SMS e mensagens no WhatsApp. Forças de autoridade e especialista em cibercrime explicam como evitar cair na 'rede'

// PÁGS. 2-3

Governo. Miguel Alves cada vez mais apertado até no Partido Socialista

// PÁG. 5

Isaltino Morais e Rodrigo Gonçalves, da comissão política do PSD, alvo de buscas

Isaltino Morais diz que estamos perante uma "fabulação", Montenegro admite suspender dirigente do partido

// PÁG. 4

Ucrânia assegura que não tem sido pressionada para negociar com Moscovo

// PÁG. 10

Produtora de Leonardo DiCaprio estreia filme sobre Pedrógão Grande

// PÁG. 32



A nova vida das velhas estações de caminhos-de-ferro

Umhas estavam desativadas, outras ainda funcionam, mas na companhia de hotéis, restaurantes, bares, sedes de juntas de freguesia ou ecopistas. E há mais novidades a caminho para os mais de mil quilómetros de linha desativada

// PÁGS. 12-17