FRAUDES E BURLAS FINANCEIRAS NUM MUNDO DE INTELIGÊNCIA ARTIFICIAL

MANTENHA-SE ALERTA E PROTEJA-SE

As fraudes e burlas financeiras *online* não são novidade, mas a Inteligência Artificial (IA) tornou-as mais inteligentes e difíceis de detetar. Atualmente são usadas mensagens e sítios da internet falsos, perfis de celebridades e até vozes ou vídeos de pessoas gerados por IA, que se assemelham a alguém que trabalha no seu banco, aos seus amigos ou família, para o enganar.

O contacto acontece, frequentemente, através de redes sociais, *e-mails*, chamadas não solicitadas e aplicações de mensagens que parecem legítimas.

Poderá enfrentar riscos como perdas financeiras, roubo de identidade e danos emocionais. Tenha cuidado e siga estas dicas para se manter seguro.

Mantenha-se atento às fraudes e burlas financeiras *online* que recorrem a IA,
por exemplo, usurpação de identidade, *phishing*, burlas de investimento e de seguros, e até mesmo fraudes e burlas românticas. Para saber mais sobre diferentes tipos de fraudes e burlas veja as páginas 5 a 7.

Para fraudes e burlas específicas de criptoativos consulte a ficha informativa "Fraudes e Burlas com Criptoativos: Mantenha-se alerta e proteja-se" ( ).

Identifique sinais de alerta:
aprenda a reconhecer comportamentos, mensagens ou ofertas suspeitas (ver página 2).

Proteja-se:
mantenha em segurança os seus dados pessoais (ver página 3).

Saiba o que fazer se for vítima de fraude ou burla
(ver página 4).

Sinais de alerta

Uma promessa que parece demasiado boa para ser verdade.

Uma chamada não solicitada de um número desconhecido.

Um pedido urgente de dinheiro ou informações pessoais, incluindo de alguém que se faz passar por um membro da família, um amigo ou mesmo uma figura pública.

Um pedido para assumir o controlo do seu dispositivo, descarregar uma aplicação, ler um QR *code* ou clicar num *link*.

Um pedido de informações pessoais ou dados bancários (por exemplo, palavras-passe, números de cartões de crédito, credenciais do *homebanking* ou códigos de segurança).

Um pedido de pagamento através de métodos não rastreáveis (por exemplo, criptoativos, cartões-presente, transferências eletrónicas ou cartões de débito pré-pagos).

Um endereço de *e-mail* ou *link* suspeito ou incorreto (por exemplo, erros ortográficos no *URL* ou endereços *web* invulgares).

Um anexo de uma fonte desconhecida, especialmente .exe, .scr, .zip, ou ficheiro Office com uma macro ativada (.docm, .xlsm).

Gramática ou formatação inadequadas num documento com aparência oficial, embora a IA possa permitir que os autores de fraudes mascarem estas falhas de forma mais eficaz.

Um sítio da internet com aparência legítima, mas sem detalhes de contacto verificados ou informações de registo da empresa.

Entoação que soa pouco natural, sem pausas e parece excessivamente fluente ou robótica. Preste atenção à ”clonagem de voz”, porque a fala gerada por IA também pode parecer muito real.

Vídeos em que a voz pode soar robótica ou excessivamente suave, os movimentos labiais e expressões faciais podem estar desalinhados com a fala, ou o fundo, a iluminação e as sombras podem ser inconsistentes. Estes são frequentemente vídeos gerados por IA (*deepfakes*).

Passos para se proteger

1 **Nunca partilhe informações pessoais ou bancárias:**

As empresas legítimas nunca solicitam os seus PIN, palavras-passe, credenciais do *homebanking* ou códigos de segurança por *e-mail*, mensagem, redes sociais ou chamada.

2 **Pare e pense antes de agir:**

Não se apresse a enviar dinheiro, a partilhar informações ou a clicar em *links* – os autores de burlas criam deliberadamente um sentimento de urgência (por exemplo, problemas informáticos com o seu banco, chamadas de emergência que envolvam os seus amigos e familiares, linguagem ameaçadora, etc.). Em caso de dúvida, mesmo que mínima, não aja. Termine a chamada e verifique cuidadosamente a fonte ou identidade.

3 **Verifique cuidadosamente a fonte/identidade:**

- Verifique sempre a origem das mensagens, chamadas, *e-mails* e *links*- mesmo que pareçam oficiais, provenham de um amigo ou familiar, ou mesmo de uma figura pública. Por exemplo, ligue ou envie uma mensagem à sua família e amigos utilizando um número conhecido através de um canal confiável; procure erros ortográficos, URL estranhos ou indicadores de segurança ausentes (por exemplo, verifique se o *link* inclui um "s" em "HTTPS" para garantir que o sítio da internet é seguro e verifique se existem letras adicionadas ou em falta no nome da empresa).

- Não abra *links* a partir de mensagens não solicitadas, instale apenas aplicações oficiais através de lojas de aplicações fidedignas e não digitalize QR *codes* desconhecidos.

- Combine com a sua família uma "palavra segura"- uma frase secreta que pode usar para confirmar a identidade caso alguém com uma voz familiar lhe ligue com um pedido urgente de dinheiro e afirme ser um membro da família (por exemplo, pais, irmã/irmão, filho).

- Utilize os dados de contacto verificados para entrar em contacto diretamente com a empresa ou a pessoa e nunca confie nas informações de contacto fornecidas pelo suspeito autor da fraude (por exemplo, pesquise o nome da empresa de forma independente, utilize diretórios comerciais verificados, métodos de contacto previamente confirmados). Os autores de burlas podem alegar estar autorizados ou replicar o sítio da internet de uma empresa autorizada. Verifique se foram emitidos avisos pela sua autoridade financeira nacional ou incluídos na lista I-SCAN da IOSCO (iosco.org/i-scan/). No caso dos prestadores de serviços de criptoativos, verifique se estão autorizados na União Europeia (UE) (por exemplo, consultando o registo da ESMA ( ).

4 **Preste atenção aos potenciais truques de IA:**

À medida que a tecnologia de IA avança, os golpes estão a tornar-se cada vez mais convincentes - mesmo com as melhores dicas de segurança. Se algo parecer fora do normal ou se detetar qualquer um dos sinais de aviso descritos acima, pare e reavalie.

5 **Nunca instale *software* de acesso remoto ou partilhe o seu ecrã:**

Os bancos e as instituições financeiras nunca lhe pedirão isso.

6 **Mantenha os dispositivos e as contas seguros:**

Utilize palavras-passe fortes e únicas, mantenha-as secretas e evite reutilizar as mesmas credenciais em plataformas diferentes. Ative a autenticação multifator sempre que possível. Consulte algumas dicas sobre palavras-passe aqui ( ). Mantenha o seu *software* e proteção antivírus atualizados e ativados.

7 **Tenha cuidado com oportunidades de investimento não solicitadas e limitadas no tempo:**

Se parece demasiado bom para ser verdade, provavelmente é uma fraude.

8 **Pense antes de partilhar informações nas redes sociais:**

Os grupos de *chat*, fóruns, publicações nas redes sociais e fotografias podem ser fontes valiosas de conhecimento para os autores de fraudes. Revelar demasiado sobre si ou sobre os seus investimentos pode torná-lo um alvo fácil.

O que fazer se for vítima de fraude ou burla

Pare imediatamente as transações:

Para bloquear quaisquer outras transferências para contas suspeitas e evitar perdas adicionais. Interrompa todos os contactos com os autores de burlas – ignore as chamadas e mensagens de correio eletrónico e bloqueie o remetente.

Contacte o seu banco ou entidade financeira:

Informe imediatamente o seu banco ou entidade financeira através dos canais de contacto oficiais, de modo a verificar se ainda é possível impedir ou reverter as transações.

Altere as suas palavras-passe em todos os seus dispositivos e aplicações/sítio da internet:

Os autores das fraudes compram palavras-passe divulgadas *online* e experimentam-nas em várias contas. Alterar apenas uma palavra-passe não é suficiente. Certifique-se que altera todas, para que os autores das fraudes não possam reutilizá-las.

Denuncie e alerte:

Comunique o incidente à polícia ou à autoridade nacional competente e informe a sua rede de contactos (por exemplo, amigos e familiares) para aumentar a consciencialização. Estas ações podem ajudar a protegê-lo e aos outros.

Cuidado com a fraude na recuperação de fundos perdidos:

O autor da fraude pode contactá-lo sabendo que é vítima de uma fraude anterior, alegando ser uma autoridade pública (por exemplo, polícia, autoridade fiscal ou financeira, etc.) e oferecendo-se para recuperar o seu dinheiro perdido mediante o pagamento de uma taxa. Trata-se, muitas vezes, de mais uma tentativa de o enganar. Lembre-se: ter sido vítima de fraude uma vez não o impede de ser novamente.

Autoridade Bancária Europeia, Autoridade Europeia dos Seguros e Pensões Complementares de Reforma, Autoridade Europeia dos Valores Mobiliários e dos Mercados, 2025

Luxemburgo: Serviço das Publicações da União Europeia, 2025

PDF ISBN 978-92-9407-234-4 doi:10.2853/8996882 DZ-01-25-123-PT-N

TIPOS DE FRAUDES E BURLAS FINANCEIRAS ONLINE POTENCIADOS POR IA

Esquemas de impersonação (falsificação de identidade) e *Deepfake*

Recebe uma chamada inesperada de alguém que alega ser do seu banco, uma autoridade pública (por exemplo, autoridade policial, fiscal ou financeira, etc.), um distribuidor de seguros, uma empresa informática ou mesmo um familiar. A pessoa que telefona pode pressioná-lo a transferir os seus fundos "para os manter seguros", alegando atividades suspeitas na sua conta ou questões relacionadas com a sua apólice de seguro. Podem também pedir-lhe que partilhe os seus dados bancários (por exemplo, número de cartão de pagamento, credenciais do *homebanking* ou palavras-passe), que clique num *link* ou instale um *software*, alegando que poderá resolver rapidamente o problema. O autor da chamada pode utilizar um número falso, muitas vezes idêntico ao número de telefone do seu banco para parecer legítimo (*spoofing*).

Os autores de burlas podem utilizar a IA para criar vídeos, imagens ou áudios falsos que imitam a voz (por exemplo, do seu gestor de conta ou de um familiar), o rosto (por exemplo, de uma celebridade) ou movimentos de alguém. **Isto é conhecido como "*Deepfake*".**

O que pode acontecer:

Ao mencionar dados pessoais e criar um sentimento de urgência, o autor da burla convence-o a efetuar ações não intencionadas, como enviar dinheiro para a conta, clicar num link malicioso ou instalar um malware no seu dispositivo. Ao fazê-lo, pode estar a conceder acesso direto às suas credenciais do homebanking. Com estas informações, ele pode alterar a sua palavra-passe, aceder à sua conta bancária e roubar o seu dinheiro. Lembre-se: o facto de a pessoa que efetua a chamada conhecer os seus dados pessoais não significa que seja de confiança.

Phishing e engenharia social

Recebe um *e-mail* ou mensagem que aparenta ser do seu banco ou de uma instituição financeira, alertando-o para "atividades suspeitas" na sua conta. O logótipo, o *design* e a linguagem parecem fidedignos e a mensagem pode surgir na sequência de conversas anteriores com o seu banco.
A mensagem incentiva-o a clicar num *link* para verificar a sua conta ou redefinir a sua palavra-passe. Esse *link* encaminha-o para um sítio da internet falso que parece idêntico ao seu *homebanking* . Sem se aperceber, introduz os seus dados num sítio da internet criado para roubar as suas informações pessoais.

Os autores de burlas recorrem a IA para criar mensagens de *phishing* convincentes, analisando os dados das redes sociais para identificar as vítimas e adaptar o conteúdo a cada alvo.

O que pode acontecer:

O autor da burla acede à sua conta bancária e rouba o seu dinheiro ou cria um perfil falso com os seus dados pessoais para cometer fraude.

Fraude de investimento ou de seguros

Vê um anúncio nas redes sociais ou num sítio da internet a promover uma "oportunidade de investimento por tempo limitado e com baixo risco" ou um "desconto por tempo limitado" num seguro de uma empresa conhecida.
O anúncio utiliza a fotografia de uma celebridade e recomendações que são, com frequência, falsas. Depois de demonstrar interesse, clicando no *link* ou preenchendo um formulário, é contactado e redirecionado para uma plataforma ou canal de mensagens onde recebe conselhos e documentos de aparência profissional. É incentivado a investir uma pequena quantia, seguida de somas maiores, ou a pagar o prémio do seguro para uma conta que parece ser segura.

Os autores de fraudes utilizam ferramentas de IA para tornar estas propostas ou *e-mails* falsos altamente convincentes e difíceis de detetar. Também recorrem a *bots* de redes sociais, alimentados por IA, para criar contas falsas que interagem consigo, disseminam desinformação e simulam comportamentos reais para ganhar a sua confiança e influenciar as suas decisões.

O que pode acontecer:

Depois de tentar levantar o seu dinheiro ou participar um sinistro, no caso de um seguro, o contacto deixa de responder. Descobre que a empresa não existe ou que o risco não está coberto por um seguro. Percebe, então, que enviou dinheiro diretamente para o autor de uma burla como parte de um esquema fraudulento. Infelizmente, não é possível recuperar o seu dinheiro e os seus dados pessoais e financeiros podem ser utilizados para cometer novas fraudes (por exemplo, assinar contratos em seu nome que podem levá-lo a perder ainda mais dinheiro).

Fraude romântica e burla

Foi contactado nas redes sociais, em aplicações de encontros ou por chamada/mensagem por alguém que não conhece. Essa pessoa mantém conversas frequentes, pessoais e românticas, criando confiança através de perfis falsos. Com o tempo, a conversa começa a focar-se em dinheiro ou oportunidades financeiras, como investimentos em criptoativos com promessas de retornos elevados e baixo risco. A pessoa pede-lhe para transferir dinheiro para uma conta ou orienta-o na criação de uma conta e na realização de um pequeno depósito inicial para tornar o esquema mais credível antes de o incentivar a investir mais.

Os autores de fraudes utilizam a IA para gerar perfis falsos, identificar as suas vítimas nas redes sociais/aplicações de encontros, utilizando dados que disponibilizou ou recorrem a *chatbots* para gerar mensagens.

O que pode acontecer:

O autor da burla retira o máximo de dinheiro possível, para depois terminar toda a comunicação e desaparecer. O sítio da internet ou a aplicação de investimento fraudulento são desativados, impedindo-o de aceder aos supostos investimentos. Para além da perda financeira, as informações pessoais que partilhou podem ser utilizadas para visar os seus amigos e familiares ou para roubar a sua identidade, o que lhe pode trazer consequências financeiras ou legais (por exemplo, o autor da fraude pode fazer compras, contrair empréstimos em seu nome responsabilizado-o, até prova em contrário, por dívidas ou crimes cometidos em seu nome).

Fraude em compras *online*

Depara-se com um negócio atrativo para uma compra numa loja *online*. A empresa que promove o negócio solicita que o pagamento seja efetuado fora da plataforma oficial, alegando que utiliza um "sistema de pagamento seguro", e envia-lhe um *link* para concluir a compra. Este *link* redireciona-o para uma página de autenticação bancária fraudulenta que replica o sítio da internet oficial do banco e utiliza o seu logótipo e *design*, pelo que introduz os seus dados bancários para efetuar o pagamento.

Os autores de burlas recorrem a IA para criar sítios da internet bancários falsos altamente convincentes, confirmações de encomendas e faturas. A IA ajuda-os a replicar o tom, a marca e o estilo das empresas legítimas. Em alguns casos, usam *chatbots* de IA para responder a perguntas e tornar o negócio mais credível.

O que pode acontecer:

O pagamento através de um link externo contorna as proteções da plataforma de vendas. O autor da burla obtém os seus dados de acesso à conta bancária e retira-lhe o dinheiro.