O AMOR ESTÁ NOS TRILHOS
Fotos de casamento no metrô viralizam
Marido e mulher celebram bodas em ensaio no meio de transporte que marcou relação

NA WEB

PARA ACESSAR APONTE O CELULAR PARA O QR CODE

ILUSÕES DIGITAIS

Alta nos crimes de estelionato é impulsionada por uso de IA

BRUNA MARTINS
E JÉSSICA MARQUES
gerais@oglobo.com.br

De acordo com dados do Instituto de Segurança Pública (ISP), órgão do governo do estado, crimes de estelionato apresentaram aumento inédito — este salto foi impulsionado pela tecnologia. O ISP levantou, há nove anos, 201 registros de golpes em ambiente virtual no Rio de Janeiro. Em 2023, o número total saltou para 11.485 casos.

Cada vez mais acessíveis, as chamadas deepfakes (sons, imagens e vídeos digitais que simulam a realidade) movimentam um mercado legal em franca expansão. Mas, produzidas através do uso intensivo de Inteligência Artificial, podem resultar tanto em cenas divertidas quanto em dor de cabeça. Na segunda lista se encaixa a ação de bandidos, ou cibercriminosos, que recorrem à IA para cometer fraudes.

VOZ E IMAGEM EDITADAS

Em alguns casos, uma suposta ligação de instituição financeira ou operadora de telefonia pode durar tempo suficiente para que a voz da vítima seja gravada e, posteriormente, reproduzida em outro contexto. Foi o que aconteceu em janeiro com Larissa (nome fictício), de 23 anos, estudante de enfermagem. Uma semana depois de ter feito a transferência de sua conta bancária para outro banco, a jovem começou a receber inúmeras chamadas de números desconhecidos. Desconfiada, desligava ou recusava as ligações.

Após muita insistência, atendeu uma delas, e ouviu a mensagem eletrônica pedindo a confirmação de dados pessoais para atualizar seu cadastro. O contato durou um minuto, o tempo necessário para que sua voz fosse gravada e, em seguida, usada em uma tentativa de golpe. Passados alguns dias, a mãe de Larissa recebeu uma ligação da filha — a voz era dela — pedindo R$ 700, que deveriam ser enviados por pix a uma amiga de quem ela nunca tinha ouvido falar.

— Não registramos ocorrência na polícia. Liguei para o banco e desisti da portabilidade. Também troquei as senhas e configurei meu celular para bloquear ligações suspeitas. Realmente não dava para saber que não era eu. Minha mãe foi esperta ao desconfiar — lembra a filha.

Para tentar evitar problemas como o de Larissa, uma empresária, que também prefere não se identificar, afirmou que em um mês bloqueou mais de 27 ligações de números suspeitos.

Com Marcelo (nome fictício), no entanto, o ataque veio pela rede social. Influenciador, com 20 mil seguidores, ele apareceu em seu perfil no Instagram, no último dia 5, protagonizando um vídeo de 7 segundos que levantou suspeitas. Nas imagens, está na praia, contando como ganhou dinheiro fácil com a ajuda de um investidor: os R$ 1 mil aplicados se transformaram em R$ 10 mil em cinco minutos. "Estou feliz demais", dizia a legenda, seguida por prints de conversas dele com o responsável pelo milagre da multiplicação do dinheiro, além de comprovantes bancários.

No vídeo, a voz de Marcelo, em sincronia com o movimento de seus lábios, reproduz o discurso falso — ele desmentiu o post e afirmou ter sido vítima de fraude por deepfake.

REPRODUÇÃO

Golpe. Participação real de Gabigol em podcast no fim do ano passado foi transformada em propaganda de esquema de apostas: "A fake news está ficando forte", postou o jogador do Flamengo

A EXPLOSÃO DOS GOLPES

O número de registros de estelionato no Estado do Rio vem aumentando desde 2017. De lá pra cá, as ocorrências cresceram quase oito vezes

ANO (JANEIRO A MARÇO)

Os dois piores meses da série histórica, iniciada em 2003, foram janeiro e março deste ano (registros)

Os estelionatos em ambiente virtual (internet, redes sociais, aplicativos) representam atualmente o primeiro lugar entre os locais para o crime

- Em 2023, foram **11.485** registros de estelionato em ambiente virtual, **9,4%** do total
- Em 2014, houve **201** registros de golpe em ambiente virtual, **0,58%** do total de estelionatos

LOCAL	REGISTROS
Ambiente virtual	11.485
Outros	10.657
Residência	8.035
Via pública	3.948
Estabelecimento financeiro	2.752
Estabelecimento comercial	2.109

Entre 2023 e 2024 (janeiro a março), os registros de estelionato cresceram 14,5% no Estado do Rio de Janeiro

As áreas de delegacia (Cisps) com mais registros de estelionato (janeiro a março de 2024)

35 (CAMPO GRANDE)	32 (TAQUARA)	16 (BARRA DA TIJUCA)	64 (S. J. DE MERITI)	42 (RECREIO DOS B.)
1.941	1.250	1.207	961	829

Fonte: ISP

EDITORIA DE ARTE

> *"Dentro das empresas existem recursos tecnológicos, mas não adianta se não conscientizarmos as pessoas. É como colocar cadeado na porta e deixar a chave do lado de fora"*
>
> **Alexandre Pinto,** especialista em segurança digital
>
> *"Realmente não dava para saber que não era eu"*
>
> **Larissa (nome fictício),** estudante de enfermagem que teve a voz gravada e usada em tentativa de golpe

Formas de prevenir fraudes com deepfake

> Nas configurações da rede social, verifique se seu perfil é aberto e, principalmente, se dados pessoais como e-mail, telefone e nome completo estão privados.

> Crie senhas fortes, com letras e números. Evite usar números de telefone.

> Bloqueie ligações de desconhecidos no celular.

> Registre boletim de ocorrência quando for vítima de tentativa de golpe com uso de IA.

> Evite cadastrar dados ou fotos em sites e aplicativos desconhecidos.

> Ao suspeitar de deepfake, verifique detalhes da imagem, como rosto, pele, olhos, sobrancelhas e a boca.

Fontes Lucas Cabral - Especialista em Segurança da Informação e DPO

ATÉ GABIGOL

Alexandre Pinto, especialista em segurança digital da Diferencial Tecnologia Consultoria e vice-presidente de Tecnologia do Flamengo, explica que o desenvolvimento das ferramentas permite a qualquer pessoa sem conhecimento técnico criar deepfakes.

Estrela do time da Gávea, que recentemente deu o que falar nas redes em foto (verdadeira) com o uniforme de outra equipe, o atacante Gabriel Barbosa, o Gabigol, teve o vídeo autêntico de uma entrevista sua, de dezembro do ano passado, adulterado: na versão falsa, com mais de 70 visualizações, aparece exaltando um site de apostas. No último dia 16, o jogador publicou em seu perfil a seguinte mensagem: "Em pleno 2024? Pprrt (papo reto)! A fake news está ficando forte".

— Dentro das empresas existem recursos tecnológicos, mas não adianta se não conscientizarmos as pessoas. É como colocar cadeado na porta e deixar a chave do lado de fora. O Flamengo foi dos primeiros a aderir à Lei Geral de Proteção de Dados Pessoais (LGPD) — diz Alexandre, antes de lembrar que o clube já teve perfis falsos derrubados por compartilhar imagens para enganar torcedores.

A Polícia Civil do Rio informa que não há registros de golpes com IA, apenas investigações em que a ferramenta é utilizada. A instituição recomenda que possíveis vítimas busquem a delegacia para registrar ocorrência.

— Para fazer uma imagem fake é preciso treinar a IA. O criminoso vai escolher a vítima a dedo, estudá-la. Essas ferramentas têm versão gratuita para teste, mas em geral são pagas. O bandido investe no crime visando retorno financeiro — explica Lucas Cabral, especialista em segurança de dados e IA.

Em nota, a Federação Brasileira de Bancos (Febraban) afirmou estar ciente desse golpe e de suas variações: "A Febraban alerta que se trata de golpe de engenharia social, que usa técnicas para enganar o indivíduo para que ele forneça informações confidenciais, como senhas e números de cartões, e, principalmente, induzir a pessoa a realizar transações financeiras para o golpista". A Febraban aconselha que as pessoas, ao receberem uma ligação suspeita, desliguem e busquem os canais oficiais de seu banco.

— Deepfake, quando utiliza imagem de menor de idade em cena de conteúdo sexual, ou de um maior de idade sem consentimento, é crime. Também é crime quando é utilizada como meio da prática de crime financeiro, enquadrada como fraude eletrônica, com punições que podem ir de quatro a oito anos de prisão — afirma Rafael Kullmann, presidente da Comissão de Crimes Digitais da OAB/RJ.