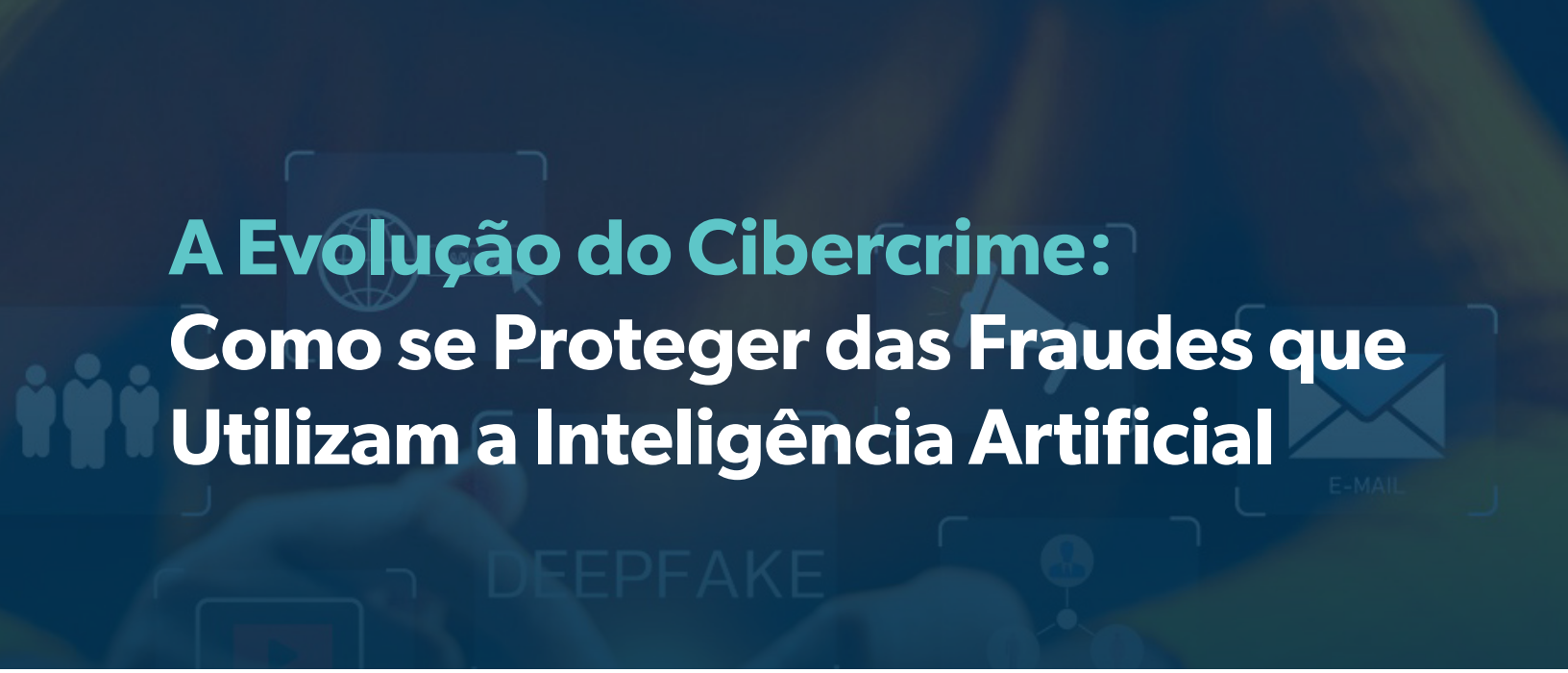

A Evolução do Cibercrime: Como se Proteger das Fraudes que Utilizam a Inteligência Artificial

À medida que a tecnologia de Inteligência Artificial (IA) evolui, também evoluem as táticas dos criminosos. Deepfakes — antes uma novidade — agora são utilizados como armas em ataques altamente convincentes por telefone (vishing).

Um artigo recente do The Wall Street Journal destaca um caso infelizmente comum — um membro da família está em perigo e precisa urgentemente de dinheiro. Porém, como revela o artigo, o familiar não está em perigo; trata-se de um golpista buscando explorar as emoções da vítima.

Em março, a Federal Trade Commission, nos EUA, divulgou dados mostrando que consumidores perderam mais de US$12,5 bilhões em fraudes em 2024, um aumento de 25% em relação a 2023. Nesses dados, a perda mediana em golpes por telefone foi de US$1.500, sendo os golpes em mídias sociais os que causaram maiores perdas totais (US$1,9 bilhões).

Martin Narcisso e David Burroughs, da StoneTurn, utilizam as lições aprendidas em muitos anos conduzindo investigações de golpes e fraudes para elencar alguns sinais de alerta e formas de proteção contra as táticas em constante evolução:

Sinais de Golpes e Fraudes

- **Falta de comunicação oficial:** Agências governamentais e forças policiais quase nunca telefonam, enviam mensagens de texto ou e-mails sem motivo prévio estabelecido com o indivíduo. Se algo parecer suspeito, sempre verifique de forma independente a autenticidade ligando para a agência pelo número listado em seu site oficial. Além disso, em e-mails, vítimas podem notar um endereço "estranho", com caracteres extras ou substituídos, ou proveniente de domínios não oficiais (por exemplo, provedores de emails pessoais).

- **Urgência:** Criminosos frequentemente ameaçam as vítimas com um problema que deve ser resolvido imediatamente (como um mandado de prisão), criando urgência para impedir que a vítima raciocine adequadamente sobre a situação. Isso também pode levar a pessoa a revelar involuntariamente informações pessoais, como nomes próprios ou de familiares, que podem ser usadas posteriormente pelo golpista.
- **Alegações impossíveis:** Os golpes muitas vezes envolvem alegações falsas — ou impossíveis — para estimular ações imediatas da vítima. Por exemplo, números de registro (como o CPF no Brasil) não expiram nem requerem pagamento para renovação.
- **Cenários anormais:** Golpistas frequentemente solicitam métodos de pagamento suspeitos para resolver uma questão, como criptomoedas ou transferências bancárias expressivas. No Brasil, são cada vez mais comuns os golpes nos quais a vítima é instruída a fazer pagamentos via Pix para terceiros.
- **Comunicação não profissional ou com falhas:** Erros de digitação, falhas gramaticais, saudações genéricas, endereços de remetente incomuns ou imagens de baixa qualidade são sinais típicos de fraude.
- **Anexos suspeitos:** Nunca abra anexos (planilhas, documentos) ou clique em links que não eram esperados. Estes podem conter malware ou redirecionar para sites maliciosos que roubam dados pessoais.

Deepfakes adicionam uma camada adicional

Com o aumento das fraudes impulsionadas por tecnologia, particularmente IA, é essencial desconfiar de fotos, vídeos ou áudios que parecem reais, projetados para induzir ações rápidas, sem validação prévia. Existem ferramentas gratuitas que podem criar deepfakes convincentes com poucos segundos de voz ou uma única foto.

Como em outros tipos de golpe, criminosos tentam extrair informações sensíveis, dinheiro ou acessos a sistemas usando intimidação e urgência.

Mais do que nunca, evoluções tecnológicas exigem que estejamos vigilantes para identificar o uso malicioso dessas plataformas.

Ações para se Proteger:

- **Monitore sua presença online:** Seja cuidadoso com as informações compartilhadas nas redes sociais, inclusive fotos que possam identificar sua localização por geo-tagging. Ferramentas de modelos de linguagem avançados (LLM) conseguem determinar com precisão a localização exata onde fotos foram tiradas, mesmo com dados limitados. Imagens aparentemente inocentes podem ser valiosas para criminosos. Restrinja as informações públicas e controle quem acessa seu conteúdo online.
- **Verifique pedidos inesperados:** Independentemente da urgência ou familiaridade da solicitação — pare e verifique. Se alguém diz ser um familiar, ligue ou mande mensagem por um número ou plataforma conhecida. Se for alguém "do governo" ligando, desligue e entre em contato pelo número oficial no site da agência ou órgão.
- **Confira links e endereços de e-mail:** Busque alterações sutis em domínios de e-mails ou links (por exemplo, "rnicrosoft.com" em vez de "microsoft.com", "gnail.com" em vez de "gmail.com") e outras discrepâncias, como e-mails pessoais usados para enviar mensagens

aparentemente corporativas ou governamentais. Passe o mouse sobre a URL antes de clicar.

- **Cuidado com voz e vídeo:** Uma voz ou rosto conhecidos não garantem autenticidade. Se algo parecer estranho, confie no seu instinto e confirme de forma independente. Pode ser útil estabelecer um código familiar para validar a identidade ao telefone em situações suspeitas.
- **Ative autenticação multifatorial (MFA):** Mesmo com senha comprometida, a MFA oferece uma camada adicional crucial de defesa. Sempre ative quando puder. Nunca aprove solicitações MFA se não estiver ativamente tentando acessar a plataforma. Caso receba uma solicitação inesperada, redefina imediatamente sua senha para a plataforma em questão.
- **Reporte atividades suspeitas:** Se for vítima de crimes ou fraudes cibernéticas, registre a ocorrência através dos canais disponibilizados pela polícia em seu Estado. Isso auxilia na coleta de informações e possibilita investigações futuras.

Tenha cuidado com golpes na era digital — assim como a tecnologia evolui, os cenários também evoluem em complexidade e sofisticação. Ao agir preventivamente, indivíduos podem evitar danos imediatos e de longo prazo.

*This is an adaptation from the original article written in English by Martin Narciso and David C. Burroughs and can be viewed on our website **here**.*