arturszczybylo_CANVA

PROTEGER SUA EMPRESA

AS FRAUDES ESPERADAS PARA ESTE ANO: TENDÊNCIAS E COMO SE PROTEGER

À medida que a tecnologia avança, os criminosos encontram novas maneiras de explorá-la para cometer fraudes. As tendências emergentes para o próximo ano indicam um aumento preocupante nas táticas utilizadas pelos fraudadores, exigindo ações proativas das empresas para proteger os seus negócios e clientes.

Thiago Bertacchini (*)

A evolução da engenharia social impulsionada pela Inteligência Artificial está transformando o cenário das fraudes financeiras, tornando cada vez mais complexo o combate a esses crimes cibernéticos. As projeções para 2024, conforme aponta a Kaspersky, indicam que a IA será uma ferramenta fundamental para os criminosos criarem golpes cada vez mais sofisticados.

A utilização de IA para criar conteúdos falsos, como anúncios, e-mails e websites, é uma tendência preocupante. Essas ferramentas permitirão uma imitação quase perfeita de canais de comunicação legítimos, dificultando a distinção entre o que é genuíno e o que é fraudulento. Isto não só aumentará o potencial de fraude, mas também levará a uma proliferação de campanhas de baixa qualidade à medida que a barreira à entrada de criminosos diminui.

Além disso, sistemas de pagamento direto, como o PIX no Brasil, tornam-se alvos de novos golpes direcionados. A expectativa é que surjam malwares bancários específicos para esses sistemas, com o objetivo de explorar suas facilidades para cometer fraudes. A automatização da fraude, especialmente no mobile banking com o ATS (Automated Transfer System), representa um desafio adicional, permitindo que os golpes aumentem sem a necessidade de intervenção manual dos criminosos.

Para o cenário empresarial neste ano, a preparação antecipada e a adoção de soluções de segurança avançadas serão essenciais. Estar um passo à frente na detecção e prevenção dessas tendências de fraude será crucial para proteger clientes e empresas. Confira as cinco principais tendências de fraudes para 2024 e saiba como se proteger:

1 Deep Fake e Chat Bots em Engenharia Social – A conscientização sobre golpes de engenharia social tem aumentado, mas os fraudadores estão se adaptando. O uso de deep fakes e chatbots para criar áudio convincente e persuasivo é uma ameaça

towfiqu_barbhuiya_CANVA

iminente. Soluções como o FraudGPT estão sendo exploradas para organizar ataques cada vez mais sofisticados.

Para as empresas digitais é importante investir em sistemas avançados de detecção de fraudes, treinar equipes para identificar sinais de manipulação e educar os clientes sobre novas formas de ataques será essencial. A tecnologia baseada em IA contribui para o desenvolvimento de métodos avançados de autenticação biométrica, como reconhecimento facial baseado em aprendizagem profunda e sistemas de reconhecimento de voz.

Além disso, a IA generativa pode auxiliar em análises comportamentais mais precisas e granulares que as empresas podem usar para criar perfis de usuário detalhados e analisar padrões de comportamento do usuário.

2 Ferramentas de fraude e acesso remoto – Os criminosos adotam ferramentas tecnológicas para mascarar a sua identidade e obter acesso remoto aos dispositivos das vítimas. Setores sensíveis, como o bancário e os de pagamentos, correm um risco substancial com esta tendência. Os decisores precisam implementar medidas de autenticação robustas, como ferramentas que possibilitem a identificação deste modus operandi, monitorar continuamente atividades suspeitas e reforçar a segurança dos dados.

3 Ataques de Bots e Device Farm – Os fraudadores estão expandindo o uso de bots e farms de dispositivos complexos para ataques direcionados e difíceis de detectar. É necessário desenvolver estratégias avançadas de detecção de ferramentas de automação, como analisar detalhadamente o comportamento e identificar padrões incomuns.

4 Fraude de afiliados em marketing digital – O marketing digital, especialmente no Brasil, corre risco com o aumento de fraudes por afiliados falsos em busca de comissões indevidas. As empresas devem encontrar formas eficazes de verificar a autenticidade dos afiliados, adotar ferramentas de monitoramento de tráfego e estabelecer protocolos rigorosos para identificar tráfego suspeito.

5 Fraude em Criptoativos e Investimentos – O mercado de criptoativos é alvo atrativo para fraudadores, que visam roubar saldos e criar contas falsas para lavagem de dinheiro. Portanto, para 2024, vale a pena reforçar as medidas de segurança nas plataformas de investimento, como uma autenticação robusta no login e o monitoramento constante das transações, o que é crucial para mitigar esses riscos.

Africa_Images_CANVA

Para se manter à frente da fraude no próximo ano, as empresas devem criar estratégias em três áreas principais: um sistema de deteção de riscos capaz de descobrir até as táticas mais obscuras utilizadas pelos fraudadores para ocultar a sua identidade e detalhes do dispositivo, modelos de machine learning e deep learning que se adaptam continuamente às ameaças emergentes, insights da dark web para se manter atualizado sobre as novas tendências e comportamentos de fraude para medidas proativas.

A evolução do ransomware também é preocupante, pois os ataques serão mais seletivos, visando instituições financeiras e estruturas criminosas mais fluidas, dificultando ainda mais o combate a estes crimes. Por fim, a exploração de vulnerabilidades em programas de código aberto e a migração para "ataques de um dia" indicam uma mudança na estratégia dos criminosos, tornando mais desafiador identificar e combater esses ataques.

Neste contexto, as corporações precisam se preparar para a evolução da IA, pois ela aumenta consideravelmente a sofisticação desses ataques, exigindo melhoria constante nas medidas de segurança, lançando mão de tecnologias Know Your Customer e digital fingerprinting, além de conscientização por parte das empresas e dos usuários finais.

(*) - Desenvolvimento de Negócios Sênior da Nethone (https://nethone.com).