



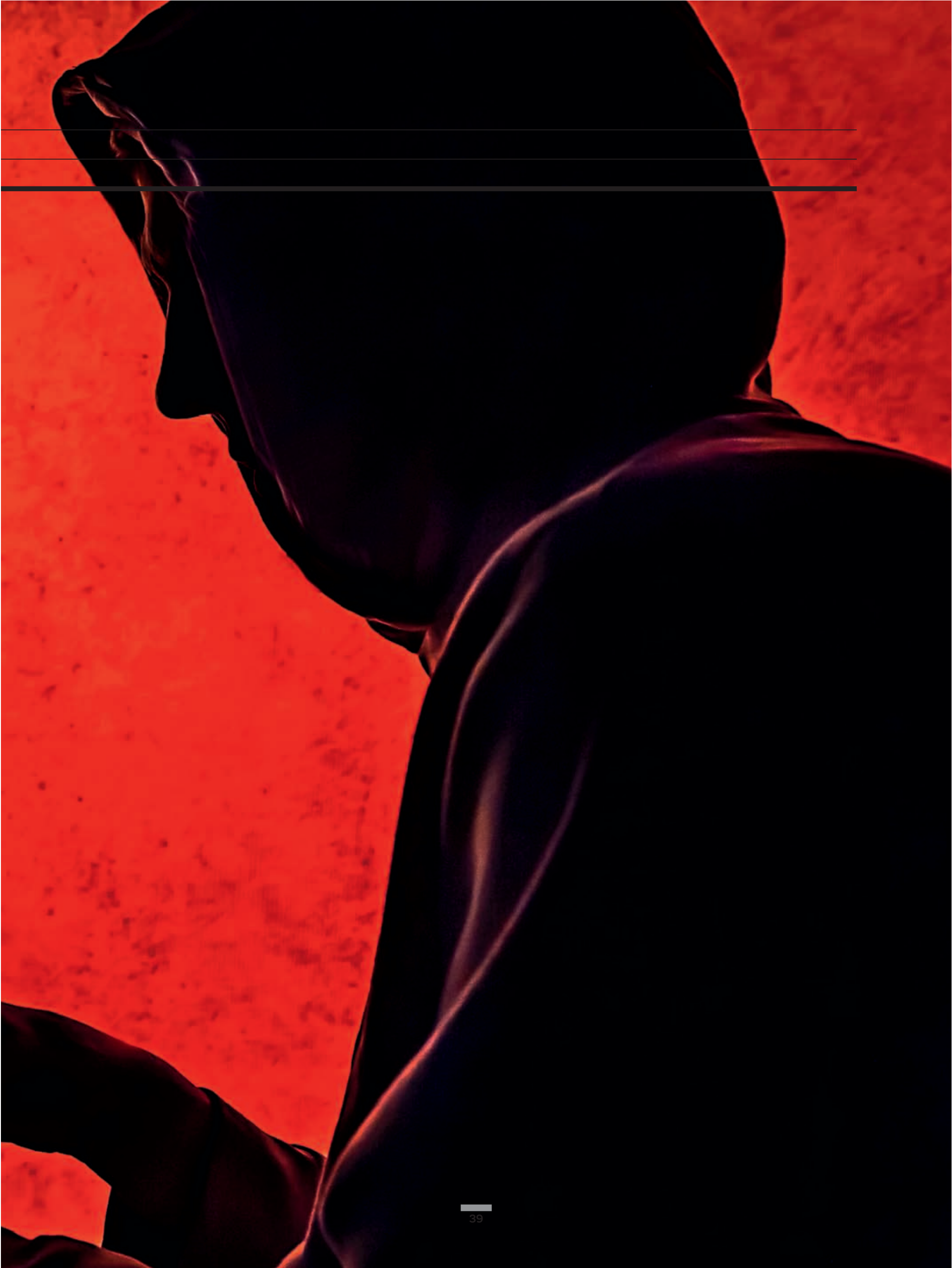
GOLPES
SET 2025

C R I M E A S A S E R V I C E

O CRIME DO SÉCULO

OS LADRÕES DE BANCO DO NOSSO TEMPO NÃO CAVAM TÚNEIS, SEQUESTRAM TRENS OU FAZEM REFÉNS. EM VEZ DISSO, TRABALHAM EM REDES GLOBAIS E USAM TECNOLOGIAS SOFISTICADAS. O CRIME DO SÉCULO NÃO VAI DEIXAR IMPRESSÕES DIGITAIS

 MARCELO MOURA





NA MADRUGADA DO dia 6 de agosto de 2005, de sexta-feira para sábado, uma quadrilha invadiu a caixa-forte do Banco Central em Fortaleza, no Ceará. Sem disparar um único tiro ou acionar qualquer alarme, carregou 3,5 toneladas em cédulas de R\$ 50 – um total de R\$ 164,5 milhões na época, o que equivale hoje a cerca de R\$ 580 milhões, segundo atualização pelo IGP-M. A Polícia Civil estimou a participação de cerca de 120 pessoas na operação, que combinou planejamento, engenharia e ousadia. O grupo alugou uma casa nas proximidades, abriu um negócio de fachada e passou três meses escavando um túnel de 80 metros até o cofre. O acesso subterrâneo foi reforçado com vigas de madeira, iluminação elétrica e até ar-condicionado, para garantir a segurança e o conforto durante o trabalho clandestino. O golpe ganhou fama de “crime do século” e virou série documental da Netflix (*3 Tonelada\$: Assalto ao Banco Central*).

Vinte anos depois, em 2025, aquele crime que parecia insuperável nem entraria na lista dos maiores golpes do semestre. No fim de junho, criminosos desviaram cerca de US\$ 1 bilhão da conta reserva que instituições financeiras mantêm junto ao Banco Central (BC). Nenhum tiro, nenhum alarme – e nenhum túnel: apenas transfe-

rências digitais instantâneas. O alvo foi a C&M Software, um Provedor de Serviços de Tecnologia da Informação (PSTI) que conecta ao sistema Pix bancos que não têm infraestrutura para isso. Em depoimento à 2ª Divisão de Crimes Cibernéticos (DCCiber) da Polícia Civil de São Paulo, um funcionário confessou ter vendido seu login e senha de acesso à rede da C&M por R\$ 5 mil, a pessoas que o abordaram quando estava saindo de um bar. Depois, recebeu outros R\$ 10 mil para desenvolver um programa que facilitou a invasão do sistema e permitiu a simulação fraudulenta de transações em nome de bancos.

O desvio de US\$ 1 bilhão foi classificado como “o maior ataque hacker ao sistema financeiro da história do Brasil” – mas quase foi superado poucas semanas depois. No fim de agosto, hackers desviaram cerca de R\$ 710 milhões, em circunstâncias semelhantes ao golpe anterior. Desta vez, o alvo do ataque foi a Sinqia, outra fornecedora de conexão ao Banco Central pelo sistema Pix. Nos dois casos, segundo as investigações, os dados e o dinheiro dos correntistas não foram afetados.

O que mudou entre o “crime do século” de 2005 e os mega-ataques hackers de 2025 foi a ascensão do *crime as a service* – o crime prestado como serviço. Essa modalidade ganhou escala com a disseminação de inovações como computação em nuvem, inteligência artificial e criptografia ponta a ponta, que democratizaram o acesso a ferramentas avançadas de computação. A evolução tecnológica, que tanto favorece cidadãos, empresas e governos, também ajuda criminosos. O marketplace do *crime as a service* é protegido por camadas de criptografia hoje acessíveis ao uso comercial: o recrutamento e a comunicação entre golpistas acontece em sigilo, por meio de aplicativos de mensagens criptografadas ponta a ponta ou comunidades na dark web. As criptomoedas funcionam como meio de pagamento ideal, permitindo remunerar colaboradores de qualquer parte do mundo.

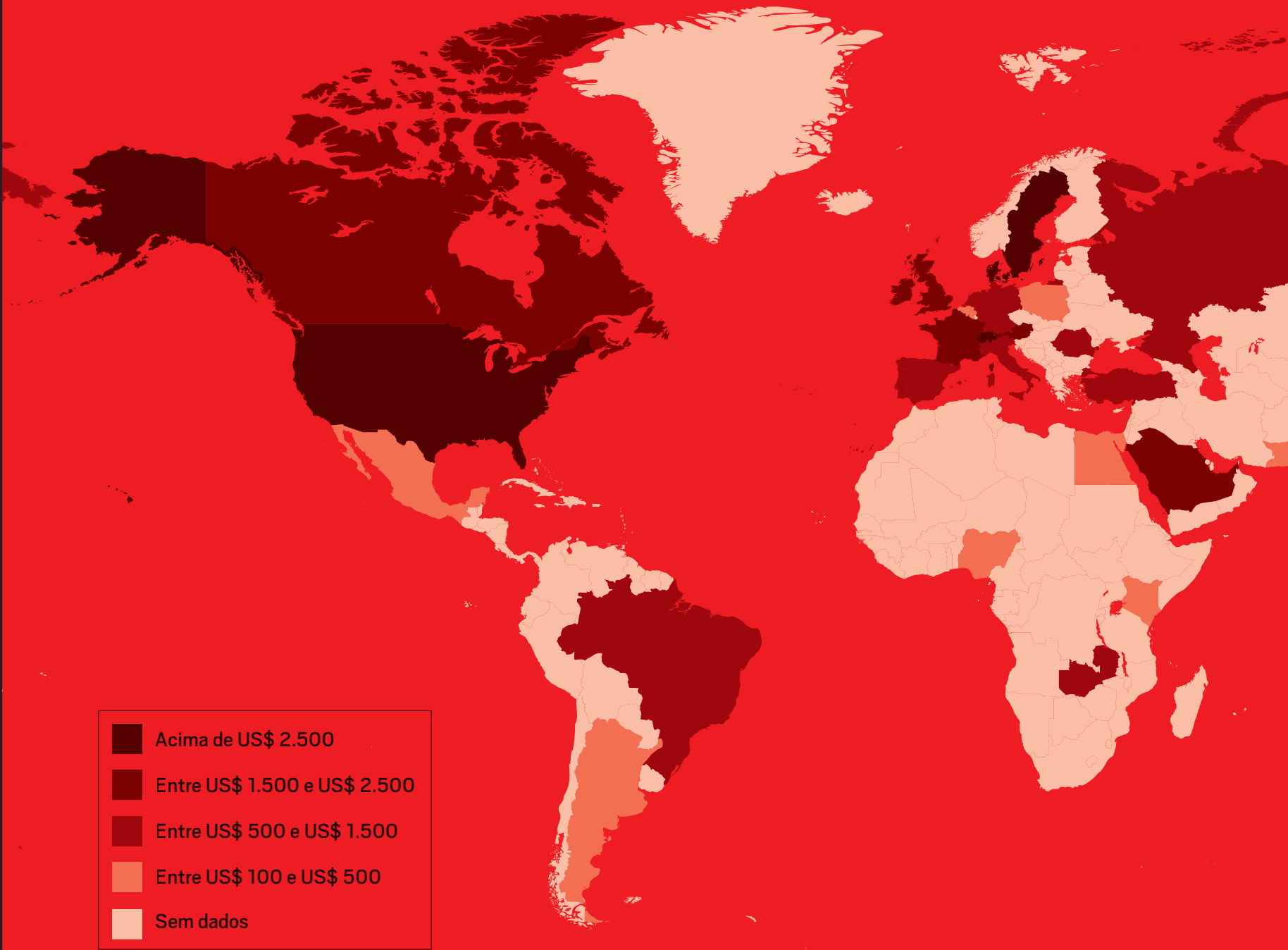
Ao facilitar a comunicação e a remuneração entre potenciais clientes e prestadores de serviço, a tecnologia transformou o crime organizado em uma indústria *asset light* – do tipo que não precisa imobilizar grandes volumes de capital para realizar seus objetivos, da mesma maneira que o Uber pode transportar milhões de pessoas por dia sem ter uma frota de carros. “Eu sou de uma geração que comprava discos. Depois veio a geração que comprava só os arquivos de música, e hoje temos uma geração que não compra nada, apenas paga pelo serviço”, afirma Roberto Rebouças, gerente geral da Kaspersky no Brasil, a ÉPOCA



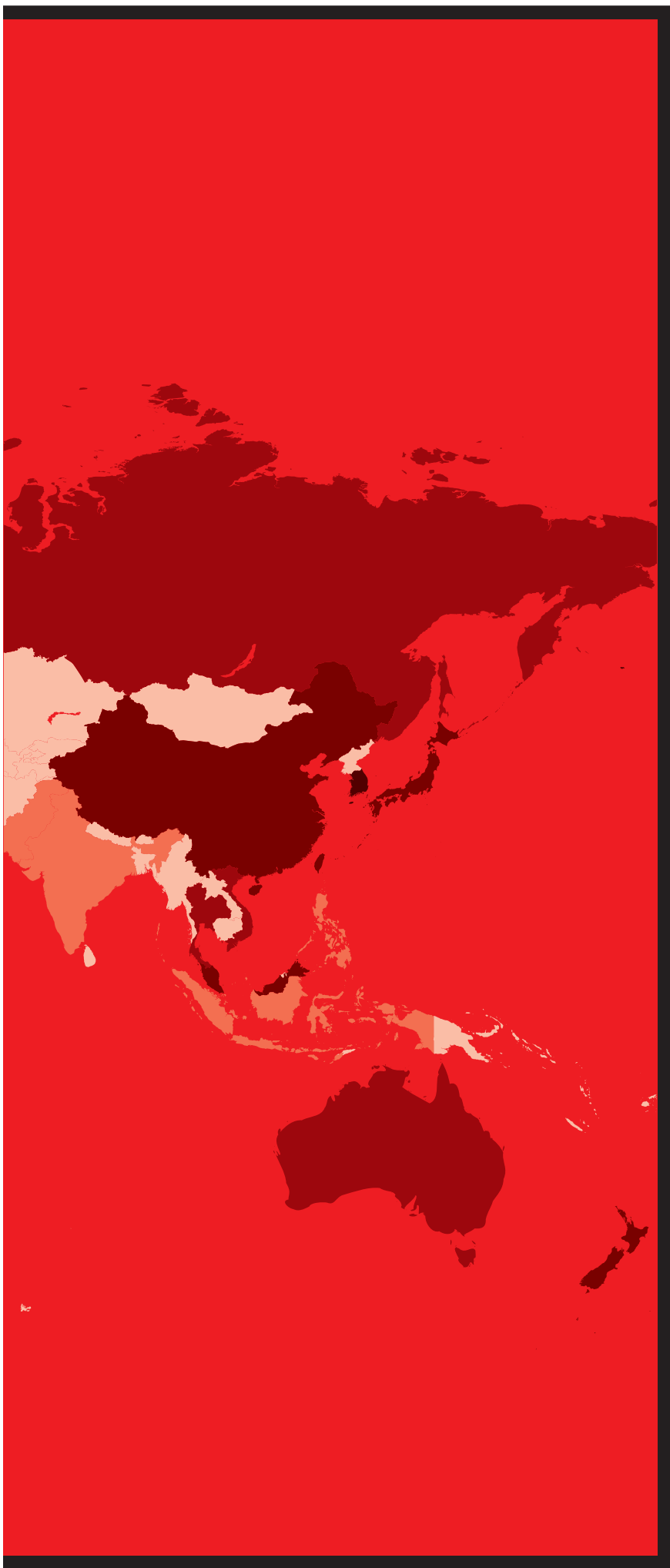
À MODA ANTIGA O elaborado assalto ao Banco Central de Fortaleza, que envolveu 120 pessoas em 2005, foi apelidado de “crime do século”

O TAMANHO DO PREJUÍZO GLOBAL

CERCA DE US\$ 1,03 TRILHÃO FOI ROUBADO EM GOLPES PELO MUNDO NOS ÚLTIMOS 12 MESES; CONFIRA O PREJUÍZO PER CAPITA DE CADA PAÍS



Estados Unidos, US\$ 3.520; Dinamarca, US\$ 3.067; Suíça, US\$ 2.980; Coreia do Sul US\$ 2.738; Suécia US\$ 2.726; Cingapura, US\$ 2.428; Japão, US\$ 2.334; Emirados Árabes Unidos, US\$ 2.194; Taiwan, US\$ 1.940; Canadá, US\$ 1.885; Nova Zelândia, US\$ 1.854; Irlanda, US\$ 1.839; Reino Unido, US\$ 1.818; França, US\$ 1.707; Arábia Saudita, US\$ 1.653; Áustria, US\$ 1.639; Hong Kong, US\$ 1.581; China, US\$ 1.578; Malásia, US\$ 1.570; Austrália, US\$ 1.452; Alemanha, US\$ 1.408; Espanha, US\$ 1.279; Tailândia, US\$ 1.106; Holanda, US\$ 938; Vietnã, US\$ 936; **Brasil, US\$ 918**; Turquia, US\$ 892; Portugal, US\$ 774; Zâmbia, US\$ 694; Rússia, US\$ 678; Romênia, US\$ 512; Itália, US\$ 512; Indonésia, US\$ 461; Polônia, US\$ 440; Índia, US\$ 384; Bélgica, US\$ 381; México, US\$ 371; Paquistão, US\$ 287; Filipinas, US\$ 275; Egito, US\$ 249; Argentina, US\$ 215; Quênia, US\$ 209; Nigéria, US\$ 119



FONTE: Global State of Scams Report 2024, GASA

NEGÓCIOS. “Com o crime digital aconteceu a mesma coisa. O criminoso não é mais aquele hacker que passa a madrugada inteira programando sozinho. Ele se tornou um empreendedor que terceiriza tarefas. Aluga ferramentas de fraude de cinco ou seis grandes grupos internacionais e encontra, dentro de empresas, funcionários dispostos a facilitar golpes em troca de uma porcentagem do ganho.”

A Organização das Nações Unidas (ONU) estima que o ecossistema do crime digital mobilize atualmente cerca de 1,5 milhão de “trabalhadores” em todo o mundo. Nem todos participam por escolha. Quem sofre um desfalque no cartão de crédito pode não imaginar, mas, muitas vezes, o golpista também pode ser uma vítima. O tráfico humano é fonte importante de mão de obra em “fazendas de golpes”. “Alguns são torturados como punição por querer deixar o local ou por não alcançar a meta diária”, disse Benedikt Hofmann, representante da UNODC (a agência da ONU de combate a drogas e crime), ao visitar um cativeiro para 700 pessoas encontrado nas Filipinas. “O Sudeste Asiático é o ‘marco zero’ da indústria global das fraudes.” De acordo com a UNODC, grandes grupos de cibercrimes exploram graus variados de ineficiência ou complacência das autoridades em países como Camboja, Mianmar, Laos, Malásia e Filipinas. A Coreia do Norte, segundo o departamento de Tesouro americano, vai além. Chega a patrocinar o Lazarus Group. O FBI acusa o Lazarus pelo maior roubo de criptomoedas da história: cerca de US\$ 1,5 bilhão da exchange Bybit, em fevereiro de 2025.

As fraudes online movimentam até US\$ 500 bilhões por ano globalmente, sendo que apenas nos Estados Unidos os prejuízos anuais somam aproximadamente US\$ 50 bilhões, de acordo com a revista britânica *The Economist*. Ainda segundo a publicação, somente em golpes de investimento envolvendo criptomoedas as perdas já passam de US\$ 6,5 bilhões anuais. A dimensão do problema tende a crescer. A consultoria Cybersecurity Ventures afirma que o número de ataques avança 20% ao ano e projeta que, em 2025, o custo global do cibercrime chegará a US\$ 10,5 trilhões – um valor que, se fosse comparado ao PIB de países, faria do cibercrime a terceira maior economia do mundo, atrás apenas dos Estados Unidos e da China. O jornal *Financial Times*, ao repercutir esse número, destacou o impacto sistêmico da “economia do crime”, capaz de afetar desde o sistema financeiro internacional até cadeias de suprimentos críticas de energia, saúde e infraestrutura.

GLOSSÁRIO DOS CRIMES DIGITAIS

ATAQUE DDOS (DISTRIBUTED DENIAL OF SERVICE)

Quando milhares de acessos artificiais sobrecarregam um site ou sistema, tornando-o indisponível para usuários legítimos.

ATAQUE DE ENGENHARIA DE PROMPT (PROMPT INJECTION) OU DATA POISONING

Manipulação de sistemas de inteligência artificial por meio de comandos maliciosos que levam a respostas incorretas, vazamento de dados ou execução de ações não previstas.

ATAQUE DE FORÇA BRUTA

Tentativas automáticas e repetidas de adivinhar senhas até encontrar a correta.

BOTNET

Rede de dispositivos infectados que passam a ser controlados remotamente por criminosos para realizar ataques em larga escala.

CRIME AS A SERVICE (CAAS)

Modelo em que ferramentas, técnicas e golpes digitais são oferecidos como serviços prontos, permitindo que qualquer pessoa contrate atividades criminosas online.

CRIPTOJACKING

Uso indevido da capacidade de processamento de computadores ou celulares de terceiros para minerar criptomoedas sem autorização.

DARK WEB

Parte da internet acessível apenas por softwares especiais, onde ocorre grande volume de comércio ilícito.

DATA BREACH (VIOLAÇÃO DE DADOS)

Exposição ou roubo em larga escala de informações sensíveis, como senhas, registros financeiros ou dados de clientes.

DEEPFAKE

Imagem, áudio ou vídeo falso gerado por inteligência artificial com aparência realista, usado em fraudes, chantagens e campanhas de desinformação.

ENGENHARIA SOCIAL

Técnica de manipulação psicológica em que criminosos exploram a confiança da vítima para obter informações ou acesso a sistemas.

EXPLOIT

Brecha ou vulnerabilidade de software explorada por hackers para invadir sistemas ou roubar dados sensíveis.

IDENTIDADE SINTÉTICA

Criação de identidades falsas a partir da combinação de dados reais e inventados, usadas para abrir contas ou obter crédito.

KEY ESCROW FRAUDULENTO

Uso malicioso de chaves de criptografia criadas originalmente para proteger informações, mas exploradas por criminosos ou insiders.

KEYLOGGER

Programa oculto que registra tudo o que a vítima digita, incluindo senhas e dados bancários.

MALWARE

Categoria ampla de softwares maliciosos criados para invadir, danificar ou roubar informações de sistemas.

MISTURADORES DE CRIPTOMOEDAS (MIXERS/TUMBLERS)

Serviços que fragmentam e reorganizam transações em criptomoedas para aumentar a privacidade dos usuários. Podem ser usados tanto para fins legítimos quanto para ocultar a origem de valores ilícitos.

MONEY MULE (LARANJA DIGITAL)

Pessoa que movimenta dinheiro de origem criminosa em suas contas bancárias ou cripto, muitas vezes sem ter consciência de que participa de fraude.

PHISHING

Envio de mensagens falsas (e-mails, SMS, WhatsApp) que imitam empresas legítimas para roubar dados ou senhas.

RANSOMWARE

Sequestro digital de arquivos: criminosos criptografam os dados da vítima e exigem pagamento para devolvê-los.

RANSOMWARE AS A SERVICE (RAAS)

Versão “industrializada” do sequestro digital: grupos criminosos elaboram e oferecem na dark web kits prontos de ransomware para aluguel, facilitando a entrada de criminosos iniciantes.

SEQUESTRO DE CREDENCIAIS

Roubo de logins e senhas, que depois serão revendidos ou usados em invasões. Também há casos em que credenciais “legítimas” são usadas por funcionários que cobram uma porcentagem por sua participação no golpe.

SIM SWAPPING

Clonagem do chip de celular para interceptar códigos de autenticação em sites e assim ter acesso a contas da vítima.

SKIMMING

Instalação de dispositivos em caixas eletrônicos ou maquininhas que copiam dados de cartões.

SPOOFING

Imitação de identidade digital (telefone, e-mail, site) para enganar vítimas e aplicar golpes.

SPYWARE

Programa que monitora a atividade de um usuário de forma invisível, coletando informações sensíveis.

SUPPLY CHAIN ATTACK (ATAQUE À CADEIA DE SUPRIMENTOS)

Quando hackers invadem fornecedores ou parceiros menores como porta de entrada para atingir uma empresa maior.

VULNERABILIDADE ZERO-DAY

Falha recém-descoberta em softwares ou sistemas, ainda sem correção, explorada rapidamente por criminosos.

WEB SKIMMING (MAGECART)

Inserção de códigos maliciosos em sites de e-commerce legítimos para roubar dados de cartões durante compras online.

WORM

Tipo de malware que se replica sozinho, espalhando-se rapidamente por redes sem necessidade de interação do usuário.



A CAPACIDADE DE GOVERNOS E EMPRESAS DE RESPONDER DE MANEIRA COORDENADA ESTÁ MUITO AQUÉM DA SOFISTICAÇÃO DAS QUADRILHAS DIGITAIS

As comparações com o tráfico internacional de drogas são inevitáveis. Mas há quem argumente que o crime digital é ainda mais nocivo. Diferentemente do narcotráfico, que depende de rotas físicas de transporte e exposição territorial, os golpes digitais podem ser executados de forma remota, em escala global e com barreiras de entrada cada vez menores. Enquanto é possível enfraquecer cartéis com a legalização de drogas associada a políticas de saúde pública, para a indústria de fraudes digitais não existe essa alternativa. Ela extrai valor daquilo que tiver valor para a sociedade. Seguir o dinheiro e condenar mafiosos por crimes fiscais, como os Estados Unidos fez com Al Capone em 1931, também está mais difícil. Operando numa zona cinzenta da legislação de muitos países, mixers de criptomoedas oferecem privacidade para transações em blockchain. Ao misturar recursos de diferentes correntistas em uma grande “piscina” e depois redistribuir, o serviço dificulta o rastreamento de fluxos financeiros – sejam eles lícitos ou ilícitos. Uma das maiores mixers do mercado, a Tornado Cash teve dois cofundadores processados por lavagem de mais de US\$ 1 bilhão em 2023.

Enquanto governos e reguladores discutem marcos legais e mecanismos de cooperação internacional, grupos criminosos já estão incorporando novas tecnologias: malwares que usam inteligência artificial para se adaptar em tempo real às defesas das vítimas, deepfakes para enganar executivos em fraudes de engenharia social. Essa assimetria se reflete nos números. Um relatório do Fórum Econômico Mundial (WEF, na sigla em inglês) de 2023 destacou que os ataques cibernéticos estão entre os dez

maiores riscos globais da próxima década, ao lado das mudanças climáticas e da crise energética. Para o WEF, a capacidade de governos e empresas de responder de maneira coordenada ainda está muito aquém da sofisticação alcançada pelas quadrilhas digitais.

O Brasil, ao mesmo tempo em que figura entre os países mais inovadores em sistemas de pagamento – o Pix é frequentemente citado pelo Banco de Compensações Internacionais (BIS) como um exemplo mundial de inclusão financeira –, também se tornou terreno fértil para fraudes digitais. O contraste é eloquente: a mesma infraestrutura que garante transferências instantâneas e gratuitas para milhões de brasileiros também permitiu que quase R\$ 1,7 bilhão fosse desviado em questão de meses por vulnerabilidades em intermediários tecnológicos. “O sistema bancário brasileiro é provavelmente o mais avançado do mundo e um dos mais seguros”, diz o diretor da Kaspersky. “O problema é que ele é só um elo numa cadeia de pessoas e empresas mais sujeitas a fragilidades.” Para evitar lavagem de dinheiro e ataques de hackers, em setembro o Banco Central impôs novas regras aos Provedores de Serviços de Tecnologia da Informação, como transferências limitadas a R\$ 15 mil e exigência de capital mínimo de R\$ 15 milhões.

Duas décadas depois do túnel de 80 metros em Fortaleza, a caixa-forte não precisa mais ser invadida fisicamente. O cofre se tornou digital e o arrombamento, silencioso. O crime mudou de escala, forma e lógica. Será que as defesas – tecnológicas, jurídicas e institucionais – conseguirão acompanhar o ritmo de inovação dos criminosos digitais? **N**



GOLPES

SET 2025

I A





MULTIPLICADORA DE GOLPES

NOS ÚLTIMOS DOIS ANOS, A IA TORNOU OS ATAQUES MAIS SOFISTICADOS E PRECISOS E TRANSFORMOU SIMPLES CRIMINOSOS EM HACKERS PROFISSIONAIS. AGORA, PREPARA-SE PARA AGIR SOZINHA, SEM NECESSIDADE DE INTERVENÇÃO HUMANA

 CLAYTON MELO





NO DIA 27 DE AGOSTO, a Anthropic informou ao público que havia detectado e bloqueado hackers que estavam usando o Claude, seu chatbot de IA, para ataques cibernéticos. O anúncio chamou a atenção de empresas, autoridades e usuários para um outro lado da regulação da inteligência artificial: sem ela, fica muito mais fácil para os criminosos avançarem de maneira exponencial na qualidade de seus golpes. Basta ver a ousadia e criatividade dos ladrões digitais. Primeiro, eles usaram a IA da Anthropic para criar e-mails de phishing altamente personalizados, escrever códigos de malware e derrubar barreiras de segurança. Depois, utilizaram o modelo de linguagem para elaborar roteiros de golpes em larga escala, para vender na dark web. Por fim, programaram o Claude Code para encontrar os melhores alvos, obter acesso às redes das vítimas, extrair dados, analisá-los e gerar uma nota de resgate.

Com esses recursos, os criminosos atacaram pelo menos 17 órgãos governamentais, organizações de saúde, serviços

de emergência e instituições religiosas, afirmou a Anthropic, sem revelar o nome dos afetados. “A operação demonstra uma evolução preocupante no cibercrime assistido por IA, que funciona tanto como uma consultora técnica quanto como uma operadora ativa, possibilitando ataques que antes seriam impossíveis”, disse em seu relatório a empresa comandada por Dario e Daniela Amodei, que baniu as contas envolvidas, rastreou as atividades criminosas e reforçou seus filtros após o assustador incidente.

Antes disso, em fevereiro, o Grupo de Inteligência de Ameaças do Google havia relatado que criminosos estavam usando o Gemini para “dar suporte a diversas fases do ciclo de vida de ataque”. Os criminosos, que o Google identificou em seu blog como sendo de países como Irã, China, Rússia e Coreia do Norte, usaram a ferramenta para geração de conteúdo, incluindo desenvolvimento de identidades e mensagens, tradução e localização. Segundo a empresa, o uso teria ficado apenas nessa camada mais superficial. “As medidas de segurança do Gemini restringiram o conteúdo que poderia aprimorar a capacidade dos adversários”, disse em comunicado. “Os cibercriminosos tentaram também invadir produtos como o Gmail, mas não tiveram sucesso”, disse o Google.

Até onde os golpes com inteligência artificial podem chegar? Os futuristas já têm a resposta: logo teremos agentes de IA capazes de abrir navegadores, extrair senhas ou escanear redes inteiras sem supervisão humana. Levando em conta as atuais vulnerabilidades das empresas – como sistemas desatualizados, credenciais fracas e processos mal configurados –, agentes de IA maliciosos não terão dificuldade para escalar seus ataques e causar danos cada vez maiores. A não ser, claro, que as companhias encontrem uma maneira de contra-atacar – talvez usando a própria IA como última defesa contra o poderoso inimigo.

Não é o caso de entrar em pânico ainda. Por enquanto, o que a grande maioria dos cibercriminosos faz é usar a tecnologia para aprimorar golpes já conhecidos, tornando-os mais convincentes, automatizados e eficientes. De 2023 para cá, o número de e-mails de phishing incrementados com IA duplicou (de 5% para 10% do total), segundo o relatório Data Breach Investigations Report, da Verizon. Faz sentido, já que foi naquele ano que os criminosos se deram conta do poder da IA generativa para atingir seus

elena is making the New Year special with her once-in-a-lifetime deal!
Click below and claim your FREE Le Creuset set before it's too late!



TrendTorch
Sponsored
Library ID: 1311782059535622

I'm back again with another crazy giveaway from Le Creuset - This time we're giving away FREE cookware sets!

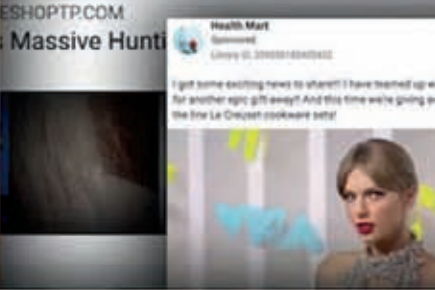


Health Mart
Sponsored
Library ID: 359058183405432

I got some exciting news to share!!! I have teamed up with Le Creuset for another epic gift-away!! And this time we're giving away some top of the line Le Creuset cookware sets!



Enter the Ravin R26X Giveaway and secure your chance to win a game-changing crossbow. Take your hunting game to the next level!



Don't rely on size and strength to prevent bad situations from happening. Instead, rely on yourself and your abilities.



IA E CIBERSEGURANÇA: A PERCEPÇÃO DAS EMPRESAS

COMO AS COMPANHIAS ENXERGAM A RELAÇÃO
ENTRE GOLPES E IA GENERATIVA



66%

das empresas
preveem que a IA
terá um impacto
mais significativo
na cibersegurança
em 2026

37%

das companhias
relatam ter
um processo
implementado para
avaliar a segurança
das ferramentas de IA

69%

das pequenas
empresas não têm
projetos para a
implantação segura
de IA; nas grandes,
esse índice é de 41%

47%

das organizações
relatam que sua maior
preocupação é o
aperfeiçoamento dos
métodos utilizados
pelos criminosos

FONTE: "Global Cybersecurity Outlook 2025", feito em
parceria pelo Fórum Econômico Mundial e a Accenture

objetivos. Embora, em teoria, o recém-lançado ChatGPT tivesse salvaguardas que impediriam seu uso em crimes, ainda em 2023 um hacker anunciou o lançamento do WormGPT, um programa que se autointitulava "IA para criminosos", por ser capaz de usar uma LLM de código aberto para remover barreiras de proteção. O programa não durou muito, mas a proposta foi abraçada pela indústria do crime digital.

Para além dos e-mails convincentes, a IA provou o seu valor para o submundo hacker ao reforçar ataques de ransomware com vídeos e áudios perfeitos, capazes de enganar até mesmo colegas de trabalho de longa data.

Não à toa, os ataques globais de "phishing de voz" cresceram 442% no segundo semestre de 2024, de acordo com a CrowdStrike. Outro estudo, do Entrust Cybersecurity Institute, dá conta de que, no ano passado, houve uma tentativa de deepfake a cada cinco minutos. "O surgimento da IA generativa aumentou significativamente a escala e a sofisticação do crime cibernético, especialmente o roubo de identidade e a fraude", diz Blake Hall, cofundador e CEO da ID.me, uma empresa americana de carteiras digitais, no site do Fórum Econômico Mundial. Ladrões digitais também passaram a explorar a IA para aprimorar os algoritmos capazes de decifrar senhas,

COMO REDUZIR OS CUSTOS DAS VIOLAÇÕES DE DADOS

O USO DA IA DE FORMA SEGURA PODE REDUZIR AS DESPESAS COM VIOLAÇÕES

R\$ 7,19 MILHÕES

é o custo médio de uma violação de dados no Brasil; valor é 6,5% mais alto do que em 2024

R\$ 6,76 MILHÕES

é o custo médio de violações para organizações que usam a IA de forma segura

13%

das organizações relataram violações envolvendo modelos ou aplicações de IA, enquanto 8% não sabiam se haviam sido comprometidas dessa forma

63%

das organizações violadas não possuem uma política de governança de IA ou ainda estão desenvolvendo uma

20%

das organizações relataram violações usando shadow AI – uso não autorizado de ferramentas de IA por funcionários

97%

das organizações comprometidas relataram não ter controles de acesso para IA em vigor

FONTE: Relatório anual Cost of a Data Breach (CODB), da IBM

deixando-os mais rápidos e eficazes.

Impulsionado pela inteligência artificial, o cibercrime desafia a economia global e a operação das empresas. Uma pesquisa da consultoria de cibersegurança Cybersecurity Ventures projeta que os custos globais com crimes cibernéticos devem alcançar US\$ 10,5 trilhões neste ano. No Brasil, o problema vem pesando no caixa das empresas. O custo médio de uma violação de dados chegou a R\$ 7,19 milhões em 2025, um aumento de 6,5% em relação ao ano anterior, segundo o relatório Cost of Data Breach (CODB), da IBM. “Um dos fatores para esse crescimento foi o uso da IA pelos criminosos, levando em conta que

ainda não existe uma proteção madura contra o uso dessa tecnologia no cibercrime”, afirma Fernando Carbone, sócio de serviços de segurança da IBM Consulting na América Latina. Setores como saúde, finanças e serviços lideram a lista dos mais afetados, registrando custos médios de R\$ 11,43 milhões, R\$ 8,92 milhões e R\$ 8,51 milhões, respectivamente. O estudo mostra que existe uma lacuna entre a rápida adoção da IA e a falta de governança e segurança adequadas. “A ausência de controles de acessos em modelos de IA expôs dados sensíveis e aumentou a vulnerabilidade das organizações”, diz Carbone. “Empresas que subestimam esses riscos não só colocam informações

EM BREVE, TEREMOS AGENTES DE IA MALICIOSOS CAPAZES DE ABRIR NAVEGADORES, EXTRAIR SENHAS OU ESCANEAR REDES SEM SUPERVISÃO HUMANA

críticas em risco como comprometem a confiança em toda a operação.”

Phishing, ransomware, quebra de senhas e deepfakes (muitas vezes sob demanda) não são as únicas modalidades com IA já disseminadas entre os hackers. Entram no pacote também as falsificações de documentos digitais, que aumentaram 244% no ano passado, segundo estudo do Entrust Cybersecurity Institute, e o uso de identidades sintéticas, combinando informações reais e falsas para criar “pessoas” totalmente novas, usadas em fraudes. Outro ataque que pode comprometer toda a estrutura de dados de uma companhia é o data poisoning, ou “envenenamento de dados”: ele acontece quando criminosos manipulam os dados de treinamento de um modelo de linguagem, com o objetivo de corromper as informações, comprometendo as operações das empresas que utilizam sistemas de IA generativa. Segundo estudo recente da Accenture, 57% dos executivos brasileiros temem esse tipo de crime.

ESCUDO CONTRA A IA

Diante de armadilhas cada vez mais sofisticadas com uso de IA, o que as empresas devem fazer para se proteger? “A prioridade é avaliar a maturidade dos programas de segurança da companhia e entender quais são as vulnerabilidades”, diz Oscar Isaka, analista diretor sênior do Gartner. Para coibir tentativas de data poisoning, é preciso adotar uma criptografia robusta, controles de acesso rigorosos e monitoramento contínuo. Usar técnicas de anonimização, como dados sintéticos, ajuda a evitar

o vazamento de informações em modelos de linguagem. Para limitar as ameaças representadas por fornecedores, é preciso realizar uma gestão de riscos da cadeia de suprimentos, exigindo validação de segurança nos modelos de terceiros. Duas das maiores dores de cabeça dos empresários, as fraudes com deepfake e phishing, podem ser prevenidas com a adoção de autenticação multifator nos sistemas e um amplo programa de treinamento sobre IA. Mas talvez o mais importante de tudo seja desenvolver um amplo plano de resposta a partir do uso da própria inteligência artificial.

Especialistas em segurança cibernética confirmam: as mesmas tecnologias de IA que impulsionam o crime cibernético poderão ser utilizadas para fins defensivos. Sistemas automatizados de detecção e resposta a ameaças, ferramentas de análise comportamental e softwares de detecção de deepfakes estão evoluindo rapidamente. Utilizar a IA para realizar varreduras em tempo real, em busca de tentativas de fraude ou comunicações suspeitas, eleva significativamente a dificuldade – e os custos – para os invasores. Segundo o relatório Cost of Data Breach (CODB), da IBM, empresas que usaram IA como parte dos programas de proteção digital tiveram menores custos de violação de dados: R\$ 6,76 milhões, ante R\$ 7,19 milhões das restantes.

Já há gente apostando nisso: em 2024, o Itaú Unibanco investiu em 50 modelos de IA exclusivos para segurança digital. A medida gerou uma economia de mais de R\$ 60 milhões, com benefício direto a mais de 300 mil clientes,



DO ATAQUE À DEFESA Cíntia Barcelos, do Bradesco, e Victor Thomazetti, do Itaú: uso de IA em sistemas de segurança digital

segundo Victor Thomazetti, superintendente de segurança corporativa do banco. “O uso estratégico da IA tem o potencial de transformar a forma como enfrentamos os desafios de segurança digital, fortalecendo a resiliência das instituições frente aos avanços dos golpistas”, afirma Thomazetti. Para ele, uma das tendências mais promissoras é o avanço das soluções de IA que alertam os clientes em tempo real sobre comportamentos suspeitos e interações potencialmente fraudulentas.

“As políticas de segurança digital precisam contemplar a governança de IA, a auditoria contínua de modelos, a proteção de dados de treinamento e a defesa em profundidade”, diz Cíntia Barcelos, CTO do Bradesco. O banco usa inteligência artificial para fazer verificação comportamental, analisando trilhões de eventos globais para

identificar desvios em perfis de usuários e aplicações. A triagem dos dados é feita por agentes inteligentes que agrupam os alertas de riscos, explicam o que aconteceu e orientam sobre os próximos passos. “Isso reduz o tempo de resposta e evita a fadiga dos analistas”, diz Cíntia.

As medidas tomadas pelas empresas para aumentar sua proteção são absolutamente necessárias, mas nem de longe suficientes. Especialistas apontam para uma solução colaborativa que envolvesse empresas de tecnologia, fornecedores de segurança cibernética, universidades e agências governamentais de diferentes países. Uma visão coletiva e integrada tornaria mais fácil identificar ameaças e adotar as melhores práticas. Algo difícil de conseguir enquanto as maiores potências globais tiverem posições tão distintas sobre regulação, uso e domínio da tecnologia. 





POR QUE OS CIBERCRIMINOSOS PREFEREM AS CRIPTOS

A FALTA DE UMA LEGISLAÇÃO INTERNACIONAL FEZ DAS MOEDAS
VIRTUAIS UM INSTRUMENTO CONVENIENTE PARA OS CRIMINOSOS
DIGITAIS – ESPECIALMENTE OS DEDICADOS AO RANSOMWARE

 MARISA ADÁN GIL, COM REPORTAGEM DE ROBERTA PRESCOTT

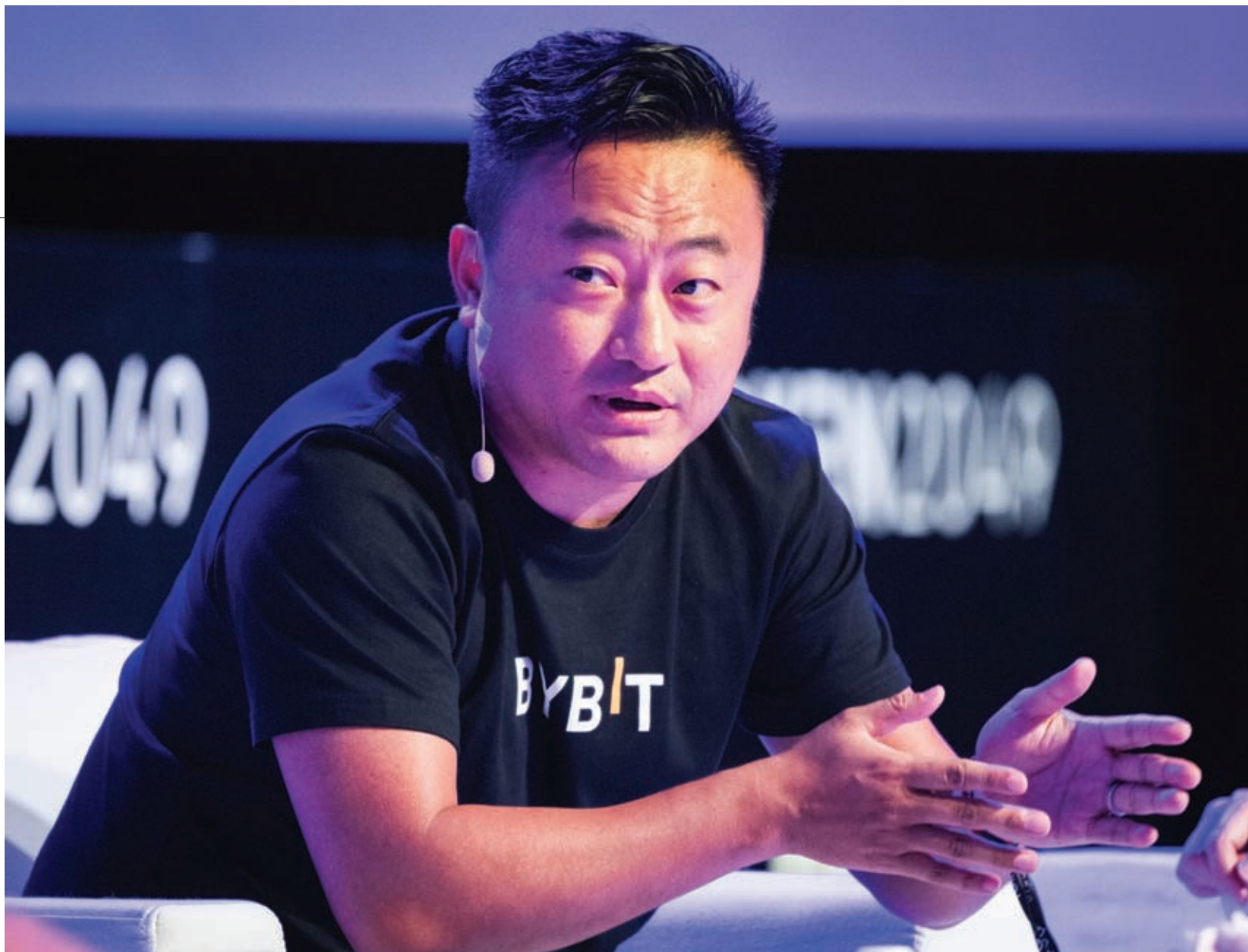


NA CIDADE DE ELKHART, no Kansas (EUA), todos consideravam Shan Hanes uma pessoa de bom caráter. Aos 53 anos, ele era o CEO do pequeno Heartland Tri-State Bank, onde eram depositadas todas as economias da comunidade local. Mas tudo mudou em dezembro de 2022, quando Hanes conheceu um “investidor” no WhatsApp que lhe ofereceu uma incrível proposta para ganhar dinheiro com criptomoedas. Se quisesse ficar rico, disse o golpista, Hanes deveria começar a depositar imediatamente os valores pedidos numa determinada conta. O que ele não sabia é que os recursos seriam enviados para carteiras de criptomoedas internacionais controladas por uma rede de criminosos. Quanto mais ele investia, mais o golpista insistia que, para liberar o retorno do investimento, seria necessário mais capital. No começo, ele usou reservas pessoais, mas depois de um tempo passou a roubar: US\$ 10 mil de um clube de investimento, US\$ 40 mil da igreja, centenas de milhares desviados do banco onde trabalhava. Talvez seu ponto mais baixo tenha sido usar US\$ 60 mil de um fundo para a faculdade da filha. No total, ele acabou transferindo US\$ 47,1 milhões para os ladrões. Em 2024, Hanes se declarou culpado de apropriação indébita bancária e foi condenado a mais de 24 anos de prisão.

No vasto oceano dos crimes envolvendo criptomoedas, a tragédia de Shan Hanes pode parecer um mero detalhe. Mas é de histórias assim que são compostos os bilhões roubados todos os anos de cidadãos comuns, que vão parar nas mãos de poderosos grupos criminosos. O ano de 2025 já estabeleceu um novo recorde em crimes digitais envolvendo criptomoedas: o ataque hacker à corretora Bybit, de Dubai, que rendeu aos criminosos do Lazarus Group, notório grupo hacker da Coreia do Norte, tokens digitais no valor de cerca de US\$ 1,5 bilhão. Segundo Ben Zhou, CEO da corretora, os ativos em ether foram retirados de uma “carteira fria”, armazenada offline e, portanto, supostamente mais segura. O roubo bilionário deve fazer com que o total de 2025 chegue ao dobro do ano anterior, quando os ataques com criptomoedas haviam somado mais de US\$ 2 bilhões. O caso da Bybit vem se juntar a outros crimes envolvendo grandes quantias de dinheiro: o roubo de US\$ 610 milhões, em agosto de 2021, da Poly Network, uma plataforma que facilitava transações de tokens ponto a ponto; os US\$ 540 milhões desviados de um projeto de blockchain vinculado ao game *Axie Infinity*, da Ronin Network, em março de 2022; e o desvio de US\$ 530 milhões da corretora Coincheck, sediada em Tóquio, em janeiro de 2018.

De acordo com informações do 2025 Crypto Crime Report, realizado pela Chainalysis, empresa de análise de blockchain que ajuda seus clientes a gerenciarem riscos, o volume global de transações com criptomoedas para fins ilícitos em 2024 foi de US\$ 40,9 bilhões. Embora o valor seja alto, representa apenas 0,14% do total movimentado globalmente em criptomoedas em 2024. Se é verdade que muitos usam cripto em transações perfeitamente legais, seu uso como ferramenta do crime segue em crescimento. Sheyner Yàsbeck Asfóra, presidente da Associação Brasileira dos Advogados Criminalistas (Abracrim), classifica os golpes cripto em três categorias: o ransomware, no qual os criminosos invadem sistemas de empresas e “sequestram” dados, exigindo resgate em criptomoedas; golpes com phishing e engenharia social, que usam links e mensagens falsas para obter acesso a dados ou induzir vítimas a transferirem ativos; e pirâmides financeiras, operações fraudulentas de investimento nas quais os pagamentos aos investidores são feitos com o dinheiro de novos participantes.

O ransomware, de longe o crime mais praticado, pela facilidade de receber o resgate em cripto, teve um crescimento de 11% em 2024, segundo a Sygnia Cybersecurity Services. O relatório anual *The State of Ransomware 2025*,



RECORDE Ben Zhou, CEO da corretora Bybit: vítima de roubo de tokens digitais no valor de cerca de US\$ 1,5 bilhão, o maior da história

da Sophos, mostra que quase 50% das empresas ao redor do mundo – e 66% das companhias brasileiras – pagaram para recuperar as informações sequestradas em 2024. Segundo o relatório global, o pagamento médio do resgate foi de US\$ 1 milhão. No Brasil, o valor médio foi de US\$ 400 mil. O Ransomware.re, um rastreador de pagamentos de resgate que monitora carteiras de cripto, calcula que, só em 2025, US\$ 62 milhões já foram pagos de resgate em todo o mundo. Pode parecer uma fortuna, mas esse montante nem de longe representa a totalidade, segundo Fabio Assolini, diretor da Equipe Global de Pesquisa e Análise da Kaspersky para a América Latina. Muitas vítimas não tornam os ataques públicos, diz, nem revelam o valor dos resgates.

“O advento das criptomoedas permitiu o crescimento exponencial dos ataques de ransomware”, diz Assolini. Desde 2019, a Kaspersky observa que, no lugar de investidas individuais, os crimes passaram a ser feitos por grupos especializados, que selecionam as vítimas e, após instalar o ransomware, chegam a monitorar a atividade econômica para calcular o valor de resgate. Divulgado em maio último, o relatório Kaspersky Digital Footprint Intelligence (DFI) revelou um crescimento de 69% dos ataques de ransomware direcionado a empresas no Brasil em 2024:

105 organizações foram atingidas, ante 62 em 2023. “O uso de cripto facilita a transferência internacional, já que boa parte dos criminosos está na Rússia, China, Coreia do Norte ou Ucrânia”, diz Daniel Molina, vice-presidente para a América Latina da iProov, empresa de segurança que fornece soluções de identidade biométrica.

FERRAMENTA DE TROCA

O início da associação entre criptomoedas e golpes digitais remonta a 2010, pouco depois do lançamento do bitcoin – não demorou muito para os hackers descobrirem o potencial da criptomoeda para fazer transações na dark web, pedir resgates e perpetuar fraudes. Durante um bom tempo, a criptomoeda original foi a mais usada pelos ladrões virtuais. “Ao se dar conta de que o bitcoin era mais rastreável que outros ativos, os hackers passaram a diversificar”, diz Assolini, da Kaspersky. O foco foi para as stablecoins, por conta da sua alta liquidez e valor mais estável, e para as criptomoedas de código aberto e voltadas para transações privadas, como a Monero. Mais recentemente, grupos de cibercriminosos passaram a oferecer o serviço “mixer”, que fragmenta e reorganiza transações em criptomoedas para dificultar o seu rastreamento.



MAIORES ATAQUES O game *Axie Infinity* e a corretora Coincheck foram alvos de dois dos maiores golpes com criptomoedas da história

A pergunta que fica é: por que, afinal, as moedas digitais se transformaram em ferramenta para os golpistas? Para começar, há a percepção do anonimato, uma vez que as transferências podem ser feitas por meio de carteiras digitais, sem o compartilhamento ou o armazenamento de dados pessoais. Outras facilidades para os criminosos são a rapidez da transação e, principalmente, a falta de uma legislação internacional única. “A criptomoeda não é regulamentada globalmente. A lei que se aplica no Brasil não vale para América Latina, Europa, Estados Unidos ou Ásia. Isso torna tudo mais fácil para o crime organizado”, diz Leidivino Natal, CEO global da Stefanini Cyber, provedora de soluções de segurança cibernética. “Todos os grupos globais de hackers usam criptomoedas como meio de recebimento”, diz André Carneiro, diretor-geral da Sophos no Brasil.

Há quem prefira não associar o uso de criptomoedas ao mundo dos crimes digitais. “É preciso acabar com a ideia de que criptomoedas facilitam golpes”, diz Bernardo Srur, CEO da Associação Brasileira de Criptoconomia (ABcripto). Ele argumenta que o uso dos ativos não é realmente anônimo: moedas digitais como bitcoin, ether e USDT operam com a tecnologia blockchain, que registra, de forma pública, imutável e auditável, todas as transações feitas. “Isso significa que qualquer movimentação deixa um histórico permanente. Mesmo em ativos mais voltados à privacidade,

como Monero, existem mecanismos para isso. Além disso, as investigações forenses têm evoluído rapidamente para identificar padrões suspeitos”, diz o executivo.

Fabrizio Tota, diretor de novos negócios do Mercado Bitcoin (MB), vai na mesma linha. “O blockchain é transparente por natureza. Com ferramentas adequadas de análise, é um grande aliado nas investigações, e tem sido cada vez mais usado por autoridades no Brasil e no mundo”, afirma o executivo. Ele usa como exemplos as prisões de Ross Ulbricht, criador do Silk Road, famoso mercado da dark web, e do casal Ilya Lichtenstein e Heather Morgan, hackers especializados em lavagem de dinheiro que foram incriminados por trilhas deixadas em blockchain. “Estamos falando de um falso anonimato. Você pode criar uma carteira sem se identificar, mas, a partir do momento em que quiser executar a transação de crypto para dinheiro fiduciário, a exchange vai pedir os dados pessoais”, afirma Caio Motta, da Chainalysis.

Polícia e empresas de cibersegurança têm aprimorado sua capacidade de monitorar carteiras de criptomoedas para saber de onde vieram e para onde vão os ativos – e agir no momento em que a crypto é convertida em dinheiro. “O caminho mais tradicional e com mais liquidez é por meio das exchanges; e elas têm todos os protocolos para barrar dinheiro que vem de fraude”, diz Sarah Uska, analista de criptoativos do Bitybank, banco digital especializado em criptoativos. “Tem casos que

CRIMINOSOS NOTÓRIOS

ELES FICARAM FAMOSOS POR SUAS ATIVIDADES
ILÍCITAS COM CRIPTOMOEDAS



SAM BANKMAN-FRIED

Em 2023, foi condenado a 25 anos de prisão por seu papel no colapso da corretora FTX. Além de lavagem de dinheiro e conspiração, foi acusado de roubar até US\$ 10 bilhões de clientes para investir em projetos pessoais.



ROSS WILLIAM ULBRICHT

Ulbricht comandou o mercado de dark web Silk Road entre 2011 e 2013, quando a polícia fechou o site e o prendeu por transações ilícitas usando criptomoedas. Foi solto em 2025 depois de um perdão concedido por Donald Trump.



ILYA LICHTENSTEIN E HEATHER MORGAN

Em fevereiro de 2022, Ilya Lichtenstein e Heather Morgan foram presos por conspiração para lavagem de criptomoedas roubadas, avaliadas em cerca de US\$ 4,5 bilhões. As moedas seriam resultado de um ataque à corretora Bitfinex em 2016.



LAZARUS GROUP

O grupo hacker, que é associado ao regime militar da Coreia do Norte, foi considerado responsável pelos roubos da KuCoin em 2020 (US\$ 275 milhões), Atomic Wallet em 2023 (US\$ 10 milhões) e Bybit em 2025 (o maior deles, de US\$ 1,5 bilhão).



RUJA IGNATOVA

Conhecida como Cryptoqueen, criou a OneCoin, um esquema fraudulento de pirâmide financeira que tirou mais de US\$ 4 bilhões de investidores em todo o mundo. Desaparecida desde 2017, continua na lista de fugitivos mais procurados do FBI.



DO KWON

O desenvolvedor das moedas TerraUSD e Luna se declarou culpado de acusações de fraude e lavagem de dinheiro em 2025. Kwon enganou seus investidores, fazendo com que perdessem um total de US\$ 40 bilhões em 2022.



NA HORA DA TROCA Sarah Uska, do Bitybank: “As exchanges têm todos os protocolos necessários para barrar dinheiro que vem de fraude”



RASTREAMENTO Fabrício Tota, do Mercado Bitcoin, e Leidivino Natal, da Stefanini Cyber: blockchain pode ser usado para chegar aos criminosos

levam mais de um ano para serem solucionados, mas, em algum momento, o criminoso vai precisar trazer o dinheiro para o mundo real”, diz Leidivino Natal, da Stefanini Cyber.

No Brasil, o Marco Legal das Criptomoedas estabeleceu regras para o mercado de ativos virtuais, com foco na proteção dos investidores e na definição de diretrizes para as empresas que atuam nesse setor. Na sequência, veio o Decreto 11.563/2023, que trouxe dispositivos para o combate a atividades ilícitas, como a tipificação do estelionato com ativos virtuais e o endurecimento das regras para lavagem de dinheiro com cripto. A legislação estabelece ainda que empresas do setor mantenham registros detalhados de suas operações e as compartilhem com as autoridades quando necessário. Falta ainda, porém, a criação de normas que complementem e detalhem a aplicação dessas leis. Quem está a cargo dessa regulamentação é o Banco Central. “A expectativa é que, quando o processo estiver finalizado, as empresas ligadas ao cripto só possam operar legalmente no país mediante autorização prévia do BC”, diz Srur, da ABcripto.

Nenhuma legislação, sozinha, é capaz de proteger as empresas. Para se precaver, é fundamental seguir com rigor as obrigações regulatórias, especialmente as estabelecidas pelo Marco Legal das Criptomoedas; adotar ferramentas de segurança, com soluções de monitoramento de blockchain como KYC (conheça seu cliente) e KYT (conheça sua transação);

e cooperar com as autoridades caso seja alvo de crimes com criptoativos. No caso das corretoras, é preciso investir em tecnologia de rastreamento e compliance, contar com sistemas de monitoramento em tempo real, realizar auditorias externas independentes, adotar governança e segregação de ativos. “O maior desafio é que grande parte das plataformas globais que operam no Brasil não seguem as boas práticas, alegando estar fora do alcance da nossa legislação”, diz Tota.

A análise dos especialistas é que a regulação brasileira avançou na criação de medidas para tentar diminuir o uso das criptomoedas em golpes, mas o ordenamento jurídico precisa andar com mais velocidade, além de garantir que as plataformas globais operem sob as mesmas regras que as locais. “Os malfeitores conhecem as corretoras que seguem diretrizes robustas de segurança e aquelas que deixam a desejar”, diz o diretor de Negócios do Mercado Bitcoin.

Golpes e fraudes envolvendo criptomoedas afetam diretamente a confiança no mercado. Por isso, o setor tem reunido esforços para atacar o uso criminoso. “O combate depende de três pilares: compliance robusto nas empresas, com identificação rigorosa de clientes e monitoramento em tempo real; regulação eficiente e clara, como o marco legal brasileiro, que garante segurança jurídica e operacional; e cooperação internacional, já que as transações são globais por natureza”, afirma Bernardo Srur, da ABcripto. **N**



GOLPES
SET 2025

S O B A M E A Ç A

EMPRESAS NA MIRA DOS HACKERS

DEEPPAKES, ROUBO DE CREDENCIAIS, PHISHING, RANSOMWARE:
ENTENDA AS PRINCIPAIS AMEAÇAS CIBERNÉTICAS E SAIBA COMO PROTEGER
AS FINANÇAS – E A REPUTAÇÃO – DA SUA COMPANHIA

 CARMEN NERY



EM JULHO DE 2024, um executivo da Ferrari recebeu várias mensagens que pareciam ter sido enviadas pelo CEO, Benedetto Vigna. As mensagens de WhatsApp, originadas de um número desconhecido, mencionavam uma aquisição significativa iminente, pediam ao executivo para assinar um acordo de confidencialidade imediatamente e alegavam que o regulador do mercado e a bolsa de valores italiana já haviam sido informados sobre a transação. Mas o tom assertivo e a foto de perfil, que mostrava Vigna em frente ao logo da Ferrari, não foram suficientes para convencer o executivo. Ele ficou ainda mais desconfiado ao receber uma suposta ligação do CEO. A voz até imitava bem o sotaque de Vigna, mas havia algumas inconsistências de estilo. Para tirar a dúvida, o executivo perguntou a Vigna qual era mesmo o nome do livro que tinha recomendado dias antes. Foi um tiro certo: na mesma hora, o golpista encerrou a ligação.

Nem todas as histórias desse tipo, porém, têm um final feliz. Grupos de criminosos cada vez mais sofisticados têm usado vozes e vídeos deepfake para roubar contas corporativas de maneira rápida e eficaz. Só nos Estados Unidos, mais de 105 mil ataques ligados a deepfake foram relatados no último ano, segundo a empresa de segurança cibernética Adaptive Security, investida da OpenAI.

Pesquisa da Kaspersky revela que um terço das empresas brasileiras sofreram golpes cibernéticos nos últimos dois anos. Além do impacto financeiro, as companhias relatam sérios danos à reputação, que podem até mesmo ameaçar a continuidade do negócio. “O ataque coloca em dúvida o nível de proteção das informações críticas, a robustez da infraestrutura e a segurança que a empresa oferece aos clientes, consumidores, parceiros e investidores”, diz Fabio Assolini, diretor da Equipe Global de Pesquisa e Análise da Kaspersky para a América Latina. “Isso se traduz em desconfiança por parte do mercado e dúvidas sobre a capacidade de a empresa operar com segurança no futuro.”

O setor de bancos e cartões continua liderando o ranking de tentativas de fraude no Brasil, concentrando 54,2% dos registros em abril de 2025, segundo pesquisa da Serasa Experian. Em seguida, aparecem serviços (30,9%), financeiras (7,2%), telefonia (5,8%) e varejo (1,9%). Para combater os criminosos, o investimento em cibersegurança das empresas brasileiras é crescente: foram R\$ 15,9 bilhões em 2023 e R\$ 18,7 bilhões em 2024 – para 2025, a projeção é de R\$ 21,6 bilhões, segundo o Relatório de Cibersegurança 2025 da Brasscom (Associação das Empresas de Tecnologia da Informação e Comunicação e de Tecnologias Digitais). Nem todo esse esforço, porém, parece suficiente para conter um dos maiores riscos empresariais: o roubo de credenciais. Em 2025, houve um aumento global de 160% no vazamento de credenciais, segundo levantamento da Check Point. No Brasil, 7,64% dos usuários no país tiveram credenciais roubadas no período analisado, a maior taxa entre todos os países pesquisados.

SEQUÊNCIA DE CRIMES

Dois ataques realizados entre junho e agosto de 2025 apontaram para vulnerabilidades na segurança do sistema Pix: em ambos, os golpistas foram capazes de movimentar quantias significativas. No primeiro golpe – o maior a atingir o sistema financeiro do país –, houve um desvio de cerca de R\$ 1 bilhão de contas de reserva que instituições financeiras mantêm no Banco Central. Tudo começou com a cooptação de um funcionário da C&M Software, empresa responsável por conectar instituições financeiras menores e fintechs ao sistema Pix do Banco Central. Primeiro, o funcionário forneceu sua senha aos bandidos; depois, ajudou a criar um sistema para permitir os desvios. O ataque do dia 30 de junho atingiu pelo menos seis instituições financeiras, entre elas a fintech BMP – que,

COMO PROTEGER SUA EMPRESA

CONFIRA AS MELHORES PRÁTICAS PARA EVITAR
OS PRINCIPAIS TIPOS DE GOLPES

1

PHISHING E ENGENHARIA SOCIAL

Treinamento contínuo

Capacite os colaboradores para reconhecer e-mails de phishing e técnicas de engenharia social.

Filtragem avançada de e-mails

Implemente soluções que bloqueiem mensagens suspeitas antes que cheguem às caixas de entrada.

Autenticação multifatorial

Adote múltiplas etapas para reduzir o risco de acessos não autorizados.

2

RANSOMWARE

Backups regulares

Mantenha cópias de segurança atualizadas e isoladas da rede principal.

Patching proativo

Aplique atualizações de segurança de forma ágil para corrigir vulnerabilidades conhecidas.

Segmentação de rede

Divida a rede em seções para limitar a propagação de malware.

3

ROUBO DE CREDENCIAIS

Autenticação biométrica

Implemente soluções que utilizem características físicas únicas para autenticação em todas as áreas da empresa.

Monitoramento de identidade

Utilize ferramentas que alertem sobre atividades suspeitas relacionadas a identidades falsas ou sintéticas.

Educação do usuário

Informe os colaboradores sobre os riscos e os sinais de roubo de credenciais, apresentando casos reais.

4

NUVEM

Segurança na origem

Adote práticas que garantam a segurança desde o início da implantação do serviço.

Controle de acesso rigoroso

Implemente políticas de acesso baseadas no princípio do menor privilégio: quanto menos acesso, melhor.

Monitoramento contínuo

Utilize ferramentas que ofereçam visibilidade em tempo real das atividades na nuvem.

5

INTELIGÊNCIA ARTIFICIAL

Soluções baseadas em IA

Implemente ferramentas avançadas de IA para detectar e responder a ameaças em tempo real.

Treinamento em IA

Capacite as equipes de segurança para entender e utilizar as ferramentas de defesa.

Avaliação contínua

Monitore e avalie o impacto da IA nas operações de segurança para ajustes contínuos.

6

TERCEIROS

Implementação de privilégios mínimos

Atribua aos usuários e sistemas apenas as permissões estritamente necessárias para suas funções.

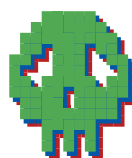
Segmentação da rede

Divida a infraestrutura em zonas isoladas, para impedir que um ataque a um parceiro se espalhe facilmente por toda a organização.

Desenvolvimento de software

Incorpore a segurança desde as fases iniciais, garantindo que bibliotecas de código de terceiros sejam monitoradas.

GRUPOS SOFISTICADOS DE CRIMINOSOS TÊM USADO VOZES E VÍDEOS DEEPPFAKE PARA ROUBAR CONTAS CORPORATIVAS DE MANEIRA EFICAZ



sozinha, perdeu cerca de R\$ 500 milhões. Mais tarde, no dia 29 de agosto, a empresa de tecnologia financeira Sinquia sofreu um ataque hacker em sua infraestrutura do Pix, com um desvio de R\$ 710 milhões de duas instituições financeiras: HSBC e Artta. Acionado a tempo, o Banco Central conseguiu bloquear parte dessa quantia. “Esse tipo de ataque, em que invasores acessam sistemas de terceiros, cresce 50% ao ano no país. Infelizmente, a maior parte das empresas não tem capacidade de investimento para monitorar agentes externos”, diz Carlos Alberto Costa, CEO da JC2Sec e diretor do Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados (IBRASPD). Para evitar lavagem de dinheiro e ataques de hackers, em setembro o Banco Central impôs novas regras aos Provedores de Serviços de Tecnologia da Informação, como transferências limitadas a R\$ 15 mil e exigência de capital mínimo de R\$ 15 milhões.

No Reino Unido, empresários sofreram em 2025 com outro tipo de crime digital, perpetrado por uma comunidade hacker conhecida como Scattered Spider. O grupo especializado em ransomware roubou os dados de milhares de clientes de varejistas britânicos como Marks & Spencer, Co-op e Harrods. De acordo com Charles Carmakal, diretor de tecnologia da unidade de segurança cibernética Mandiant, do Google, a ameaça não está

restrita à Grã-Bretanha: golpes direcionados a redes de lojas, seguindo os mesmos padrões, já estão se espalhando também pelos Estados Unidos. “Eles tendem a se concentrar em um setor específico da indústria e em uma região geográfica determinada por algumas semanas e depois mudam para o seguinte”, disse ele. As ações do Scattered Spider não são diferentes das de outras grandes redes de golpistas digitais. Hoje os cibercriminosos agem em cadeia, e muitas vezes de forma segmentada. “Eles atuam com redes estruturadas. O hacker atual é, em muitos casos, um prestador de serviço altamente especializado, oferecendo hacking sob demanda em um mercado cada vez mais robusto. O crime está mais acessível, eficiente e difícil de rastrear”, diz Allan Costa, co-CEO da ISH Tecnologia.

Em 2024, o IBRASPD identificou 66 ataques relevantes a empresas brasileiras que se tornaram públicos, com repercussão na mídia. A lista inclui Unimed, Porto de Santos, Enel, BTG Pactual, Sabesp, Vivara, Netshoes, Toyota, Marisa, Unidas e Caixa. Atacada em 22 de março de 2025, a XP tornou público o incidente um mês após o ocorrido. A empresa enviou um comunicado a seus clientes informando o acesso não autorizado a uma base hospedada em um fornecedor externo. Foram vazados três tipos de informações: dados cadastrais, informações sobre os produtos financeiros contratados e dados como o núme-

COOPERAÇÃO Mauricio Cerri, da Unimed: colaboração entre diferentes unidades para resolver incidentes e compartilhar aprendizados





O QUE FAZER APÓS UM ATAQUE



LEVANTAMENTO

A primeira ação é identificar quais informações foram acessadas e quais pessoas e processos foram impactados, para depois avaliar os custos para a empresa – financeiros e de reputação.



RECUPERAÇÃO DOS SISTEMAS COMPROMETIDOS

É preciso isolar as máquinas. Se for detectado que os invasores estão criptografando arquivos, o processo deve ser interrompido e os sistemas restaurados usando os back-ups.



ACIONAMENTO DO SEGURO

O seguro pode cobrir o resgate pago ao golpista, indenizações por danos a terceiros, despesas com escritórios de advocacia ou empresas de tecnologia.



COMUNICAÇÃO A ÓRGÃOS REGULATÓRIOS

Em caso de dados vazados, se houver risco ou dano, é preciso comunicar o incidente à ANPD e aos donos dos dados. Outros órgãos como Banco Central, CVM, Susep e agências reguladoras ajudam a evitar risco sistêmico.



TRANSPARÊNCIA SEMPRE

Por recomendação da ANPD, a comunicação deve ser em linguagem simples e clara, para compreensão do titular do dado afetado, a fim de que ele saiba que medidas de proteção tomar.



PROTEÇÕES REFORÇADAS

Faça uma análise completa de segurança para identificar as vulnerabilidades que foram exploradas pelos atacantes e revise suas políticas de segurança.

FONTE: Tiago Neves Furtado, sócio do Opice Blum Advogados

ro de conta, saldo e limite de crédito, referentes ao mês de março. Procurada pela reportagem, a XP não quis se pronunciar sobre o caso.

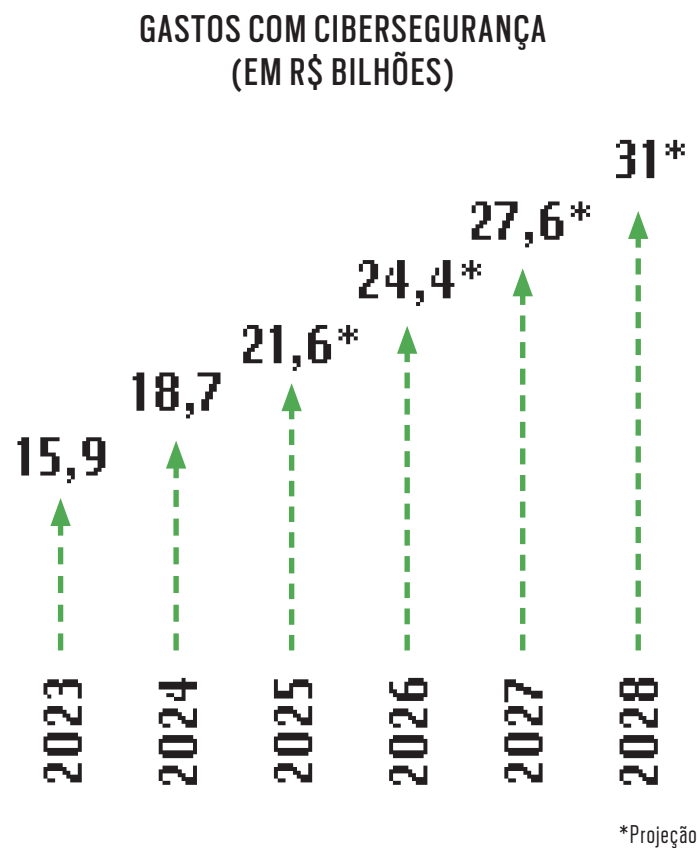
A empresa de planos de saúde Unimed teve duas de suas unidades atacadas no ano passado. Um dia depois de um crime cibernético afetar os sistemas da Unimed Cuiabá, as unidades do Vale do Taquari e do Rio Pardo (RS) também foram comprometidas, tornando os sistemas instáveis e impactando os atendimentos de urgência e emergência. Para tentar evitar novas ocorrências, a empresa criou o Programa Nacional de Governança em Proteção e Privacidade de Dados, diz Mauricio Cerri, superintendente de Tecnologia e Negócios da Unimed do

Brasil. “As unidades locais atuam de forma independente, mas quando há um incidente, procuramos entender o que ocorreu e garantir o atendimento. Como temos um processo de cooperação, organizamos os técnicos do sistema nacional para recuperar o ambiente de forma rápida e compartilhar com a rede as lições aprendidas”, diz Cerri.

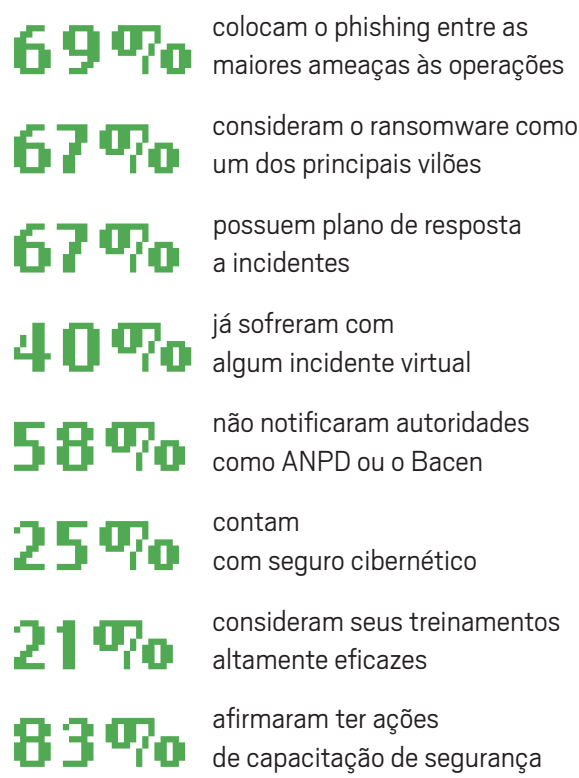
Maior porto da América Latina, Santos sofre milhares de tentativas de golpes digitais por mês, entre varreduras automatizadas, phishing, exploração de vulnerabilidades e outras ações maliciosas. Em março de 2024, o Porto foi atingido por um ataque de negação de serviço distribuído (DDoS), que consiste em uma sobrecarga proposital de acessos ao site institucional, com o objetivo de

DEFESA Anderson Pomini, da Autoridade Portuária de Santos: migração para ambiente mais robusto para evitar ataques como o do ano passado

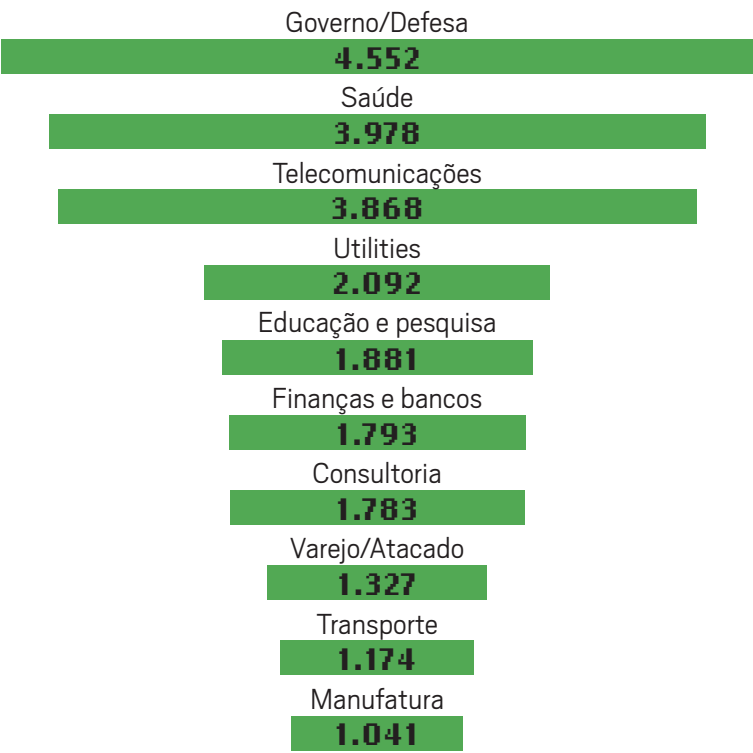
O CENÁRIO DOS GOLPES CONTRA EMPRESAS NO BRASIL



COMO AS EMPRESAS BRASILEIRAS LIDAM COM OS CRIMES VIRTUAIS

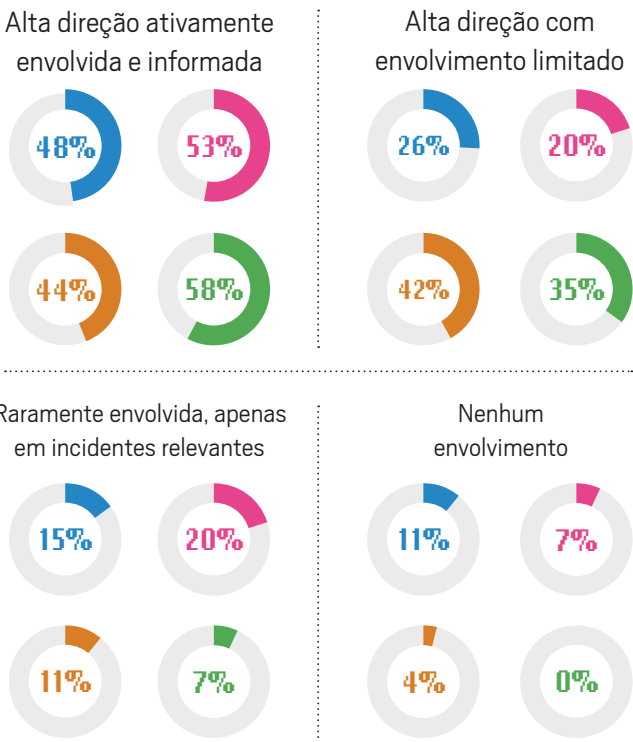


ATAQUES SEMANAIS POR SETORES EM 2024

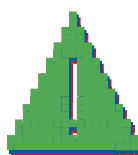


ENVOLVIMENTO DA LIDERANÇA NA PREVENÇÃO

MICROEMPRESA PEQUENO PORTE MÉDIO PORTE GRANDE PORTE



UM TERÇO DAS EMPRESAS BRASILEIRAS SOFRERAM ATAQUES CIBERNÉTICOS NOS ÚLTIMOS DOIS ANOS, COM DANOS FINANCEIROS E DE REPUTAÇÃO



esgotar os recursos do servidor e torná-lo indisponível para usuários legítimos. Segundo Anderson Pomini, presidente da Autoridade Portuária de Santos (APS), o site chegou a ficar duas horas fora do ar: só não houve mais danos porque as operações portuárias críticas de Santos – movimentação de cargas ou agendamentos – têm sistemas específicos e independentes. “A atuação da equipe técnica foi imediata, com ações de contenção, verificação de integridade e sigilo das informações, reforço de segurança e reorganização da infraestrutura”, diz Pomini. Para coibir novas tentativas de invasão, houve migração para um ambiente mais robusto, implantação de proteção adicional contra DDoS, segmentação de rede e ajustes de configuração no sistema de gerenciamento de conteúdo, além de novos treinamentos com os colaboradores. “A principal linha de defesa continua sendo a capacitação – porque a tecnologia é essencial, mas a conscientização e a preparação dos profissionais fazem toda a diferença”, diz Pomini.

Paralisação das operações por uma semana, prejuízos com resgate e atrasos na entrega foram o saldo do golpe contra a Dias+, provedora de logística last mile de carga fracionada, em plena Black Friday de 2024. A empresa atende algumas das principais marcas de cosméticos do país – entre elas Natura, Boticário, Jequití e Avon. O diretor Marcelo Dias conta que, na madrugada de 25 de novembro, os sistemas da empresa foram hackeados, com roubo de dados. Naquele primeiro dia, de forma precária, a empresa fez algumas entregas usando

planilhas e iniciou a negociação com os criminosos. “Pagamos o resgate, mas eles não devolveram nosso sistema. Tentamos outras soluções, mas ficamos sem poder trabalhar até o dia 29, quando nossa equipe de TI finalmente conseguiu trazer o nosso sistema de volta”, afirma Dias. Após o incidente, ele mudou de data center e as medidas de segurança foram reforçadas, a fim de evitar novos incidentes. “O meu alerta é: não espere acontecer algo para depois correr atrás. Contrate uma empresa de segurança, peça uma avaliação e reforce sua proteção o quanto antes”, diz o executivo.

Ao que parece, a maior parte das empresas entende que está sob ameaça constante. Realizado em 2025, o levantamento Riscos Cibernéticos – A percepção das Lideranças Brasileiras e Práticas Adotadas, da Grant Thornton em parceria com a Opice Blum Advogados, avaliou a percepção de risco de 248 empresas brasileiras de diferentes portes e setores. Quase 80% delas se consideram expostas a incidentes de segurança; 67% já têm planos de recuperação; 66,5% colocam a cibersegurança entre os cinco maiores riscos corporativos. Entre as grandes empresas, 75% enxergam como principais fatores de risco a falta de estrutura e os treinamentos. O estudo revela ainda uma nítida correlação entre o engajamento da alta gestão e a adoção de práticas mais robustas de segurança digital: 85% das empresas que realizam mapeamento e controle de riscos cibernéticos contam com o envolvimento da alta direção no tema. Nesse caso, a participação do CEO pode fazer toda a diferença. **N**

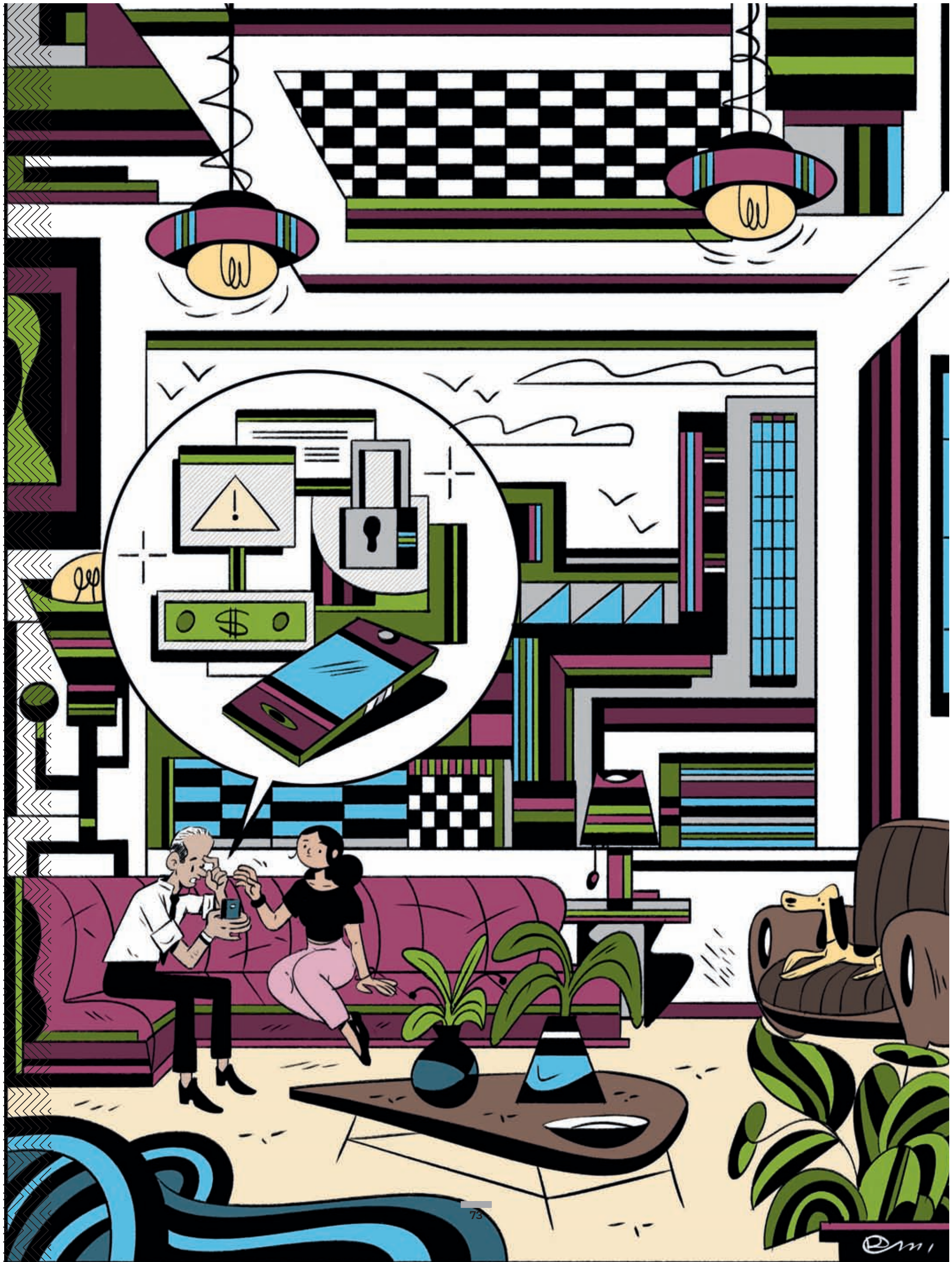


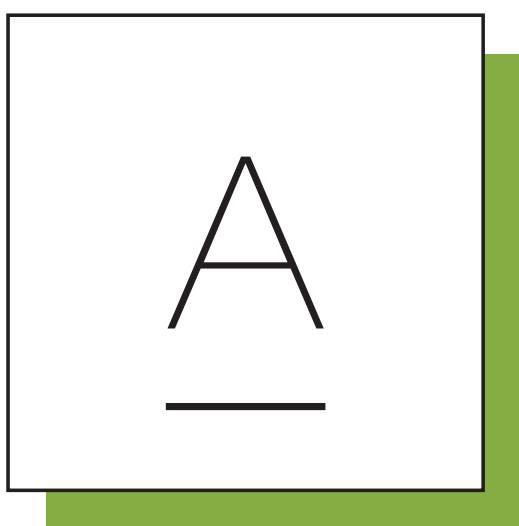
GOLPES TODOS OS DIAS

EM TODO O MUNDO, OS PREJUÍZOS CAUSADOS PELOS CIBERCRIMES EM 2024 SUPERARAM US\$ 1 TRILHÃO. NO BRASIL, 41% DA POPULAÇÃO DIZ SOFRER TENTATIVAS DE GOLPES DIARIAMENTE. COMO SE PROTEGER DA CRESCENTE INDÚSTRIA DO CRIME DIGITAL?

 DENIZE BACOCINA

ROUBO DO INSTAGRAM Golpistas tomaram controle da conta de Pedro Varone na rede social e ofereceram produtos a seus amigos





AO SER CONVIDADO a participar de um grupo de WhatsApp com dicas de investimentos, o engenheiro mecânico Adilson Pereira Lima, 55 anos, achou que havia encontrado uma boa oportunidade para ganhar dinheiro. “No começo fiquei só olhando as mensagens, mas logo vi que muitas pessoas estavam ganhando dinheiro”, conta. As primeiras dicas de ações renderam bem e ele ficou animado. Mas a bolsa de valores começou a cair e veio a sugestão de aplicação em criptomoedas. “Nas duas ou três primeiras vezes, tive ganhos exorbitantes. Daí eu caí na armadilha.” Lima investiu R\$ 60 mil, com a promessa de multiplicar o montante por seis. Na primeira semana, chegou a ver o extrato, mas na segunda o aplicativo deixou de funcionar. Ao tentar entrar em contato com os outros participantes, descobriu que, no grupo com cerca de cem pessoas, apenas ele e mais um eram investidores reais – os outros provavelmente eram chatbots. “Os sentimentos que eu tenho agora são de vergonha e tristeza. A gente sabe que isso acontece a toda hora, mas nunca acredita que vai acontecer com você”, diz o engenheiro.

Golpes sofisticados, que envolvem inteligência artificial, criptomoedas e engenharia social são exemplares de uma nova era dos ataques cibernéticos. Na última década, o cibercrime se tornou um grande negócio – uma indústria

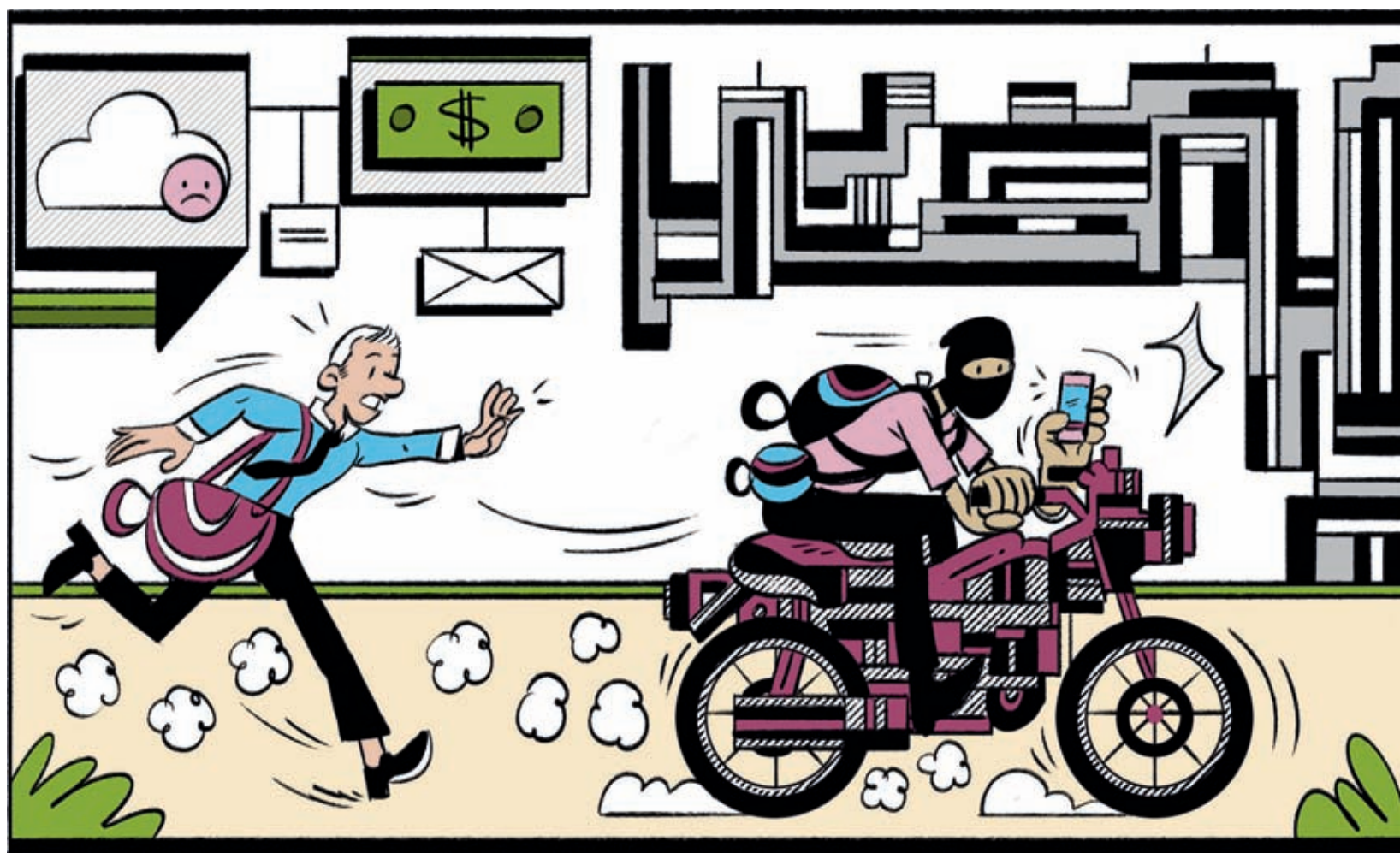
de mais de US\$ 1 trilhão, com um ecossistema inteiro de grupos criminosos administrados como se fossem empresas. Alguns até oferecem apoio técnico, instruções passo a passo e um atendimento ao cliente na dark web. Em seu relatório Global State of Scams de 2024, a Global Anti-Scam Alliance (Gasa), em parceria com a Feedzai, revelou que golpes contra empresas e pessoas físicas totalizaram US\$ 1,03 trilhão globalmente em 2024. O levantamento, baseado em insights de 58.329 entrevistados em todo o mundo, destaca os enormes prejuízos causados pelos golpes e a crescente disparidade entre as vítimas em diferentes regiões.

Cerca de 50% dos consumidores globais são alvos de ataques pelo menos uma vez por semana. No Brasil, os entrevistados relataram sofrer tentativas de golpes todos os dias. Mas enquanto países como Brasil e Coreia do Sul veem os golpes aumentarem ano a ano, outros, como Vietnã, Arábia Saudita e China, relatam uma redução acentuada nos últimos 12 meses. E embora as vítimas em países desenvolvidos como Estados Unidos, Dinamarca e Suíça sejam responsáveis por algumas das maiores perdas per capita (nos EUA, o valor médio é US\$ 3.520), é em países em desenvolvimento como o Paquistão que os prejuízos representam uma preocupação maior, com golpes representando impressionantes 4,2% do PIB do país. O impacto emocional também é enorme. Em países como Quênia, África do Sul e Filipinas, as vítimas dizem sentir-se profundamente vulneráveis, com sensações de medo e desilusão. Enquanto isso, em regiões como Japão e Coreia do Sul, embora o dano financeiro seja substancial, o impacto emocional é comparativamente menor, diz a Gasa.

No Brasil, em 2024, 24 milhões de pessoas sofreram golpes com Pix ou boletos falsos, com prejuízo médio agregado de quase R\$ 29 bilhões, segundo a Pesquisa de Vitimização e Percepção sobre Violência e Segurança Pública no Brasil, realizada pelo Datafolha em parceria com o Fórum Brasileiro de Segurança Pública. Ainda de acordo com o levantamento, 32 milhões de pessoas foram vítimas de ameaças ou chantagens decorrentes de dados vazados. O levantamento, que entrevistou 2.007 pessoas em 130 municípios, mostra a enorme abrangência e crescimento dos crimes digitais no país: entre 2024 e 2025, os golpes envolvendo Pix ou boletos falsos foram de 10,8% para 14,3% da população; as vítimas de fraude com cartão de crédito passaram de 6,7% para 8%; e a fatia dos que não receberam compras feitas em sites aumentou de 13,7% para 17,7%. Entre janeiro e junho de 2025, segundo a Serasa Experian, houve 6,4 milhões de tentativas de fraude, ou uma a cada 2,4 segundos: se todas tivessem tido sucesso, o prejuízo poderia ter chegado a R\$ 39,8 bilhões.



ENTREGA DO MAL Vítima do golpe da falsa entrega, Laerte Souza passou seu cartão de crédito na maquininha e foi roubado em R\$ 3,2 mil



ROUBO DUPLO Dilson Canovas Campos teve dois iPhones roubados com aplicativos de bancos instalados: o prejuízo foi de R\$ 7,3 mil

Assim como no resto do mundo, os golpes registrados no país são variados, e ninguém está ileso: de jovens estudantes a idosos, de pessoas com baixa escolaridade a profissionais altamente capacitados e em posições de destaque na carreira, todos são vítimas dos golpes digitais. Uma pesquisa do DataSenado no ano passado, com 22 mil pessoas, mostrou que os jovens entre 16 e 29 anos representam 27% das vítimas das fraudes, enquanto os maiores de 60 anos respondem por 16%. A diferença é que, no caso dos jovens, os golpes mais comuns envolvem compras pela internet ou redes sociais; idosos costumam ser alvos de fraudes bancárias.

Diante de um cenário tão avassalador, como o consumidor pode se proteger? A providência mais óbvia – evitar que outras pessoas tenham acesso a seus dados pessoais – é uma tarefa quase impossível, numa era em que uma rápida pesquisa na internet consegue trazer nome completo, CPF e e-mail de qualquer um, e nossos dados estão espalhados por dezenas de redes sociais, sites

de compras e serviços de streaming. Mas dá para tomar algumas providências, criando senhas fortes, utilizando aplicativos de criptografia, adotando autenticação em duas fases e biometria, entre outras.

Se é impossível impedir que os criminosos conheçam pelo menos parte dos seus dados, é bom lembrar que muitos golpes dependem de uma ação sua para se concretizar – confirmar informações pessoais, clicar num link, instalar um aplicativo, tirar uma foto. O delegado Paulo Eduardo Barbosa, da Divisão de Crimes Cibernéticos (DCCiber) do Departamento Estadual de Investigações Criminais (Deic) de São Paulo, lembra que a maior parte dos golpes trabalha com engenharia social, dados disponíveis nas redes e uma falsa noção de urgência, além de explorar sentimentos como autoridade, medo, escassez e ganância. É aí que o cidadão pode se proteger. “O golpista precisa que você faça o depósito, compre o produto ou faça o Pix imediatamente. Tudo aquilo que é urgente, é golpe”, diz o delegado.

UM TERÇO DA POPULAÇÃO JÁ SOFREU GOLPES DIGITAIS

56 MILHÕES DE PESSOAS FORAM VÍTIMAS DE FRAUDES VIRTUAIS EM 2024

24 milhões

de brasileiros foram vítimas de golpes do PIX ou de boletos falsos em 2024

19,2 milhões

foram vítimas de golpes nos quais o criminoso roubou a sua identidade

15,7 milhões

tiveram seu celular roubado ou furtado no ano passado

6,4 milhões

de tentativas de fraudes ocorreram entre janeiro e junho de 2025 no Brasil

EVOLUÇÃO DO NÚMERO DE GOLPES

Pagou por algum produto comprado pela internet ou redes sociais que não foi entregue



PREJUÍZO MÉDIO DE R\$ 446

Foi vítima de golpe envolvendo PIX ou boleto falso



PREJUÍZO MÉDIO DE R\$ 1.198

Sofreu alguma fraude de cartão de crédito



PREJUÍZO MÉDIO DE R\$ 1.690

Sofreu golpe ou fraude em algum investimento que realizou após publicidade em redes sociais ou na internet



PREJUÍZO MÉDIO DE R\$ 717

Sofreu alguma fraude bancária na conta corrente ou poupança



PREJUÍZO MÉDIO DE R\$ 3.448

*não disponível

36,3%

da população brasileira sofreu uma tentativa de golpe virtual em 2024, com ou sem prejuízo financeiro

33,4%

da população com mais de 16 anos, ou 56 milhões de pessoas, foram vítimas de fraude em meio digital com prejuízo financeiro direto em 2025

31,4%

foram vítimas de crimes virtuais com vazamento de dados ou identidade

19%

foram ameaçadas ou chantageadas depois de um vazamento de dados

Fonte: Pesquisa de Vitimização e Percepção sobre Violência e Segurança Pública, FBSP e Datafolha; Serasa Experian

OS PRINCIPAIS GOLPES VIRTUAIS PRATICADOS NO BRASIL

DIFÍCIL ENCONTRAR ALGUÉM QUE NÃO TENHA SOFRIDO PELO MENOS UM DELES



PIX OU BOLETO FALSO

A vítima recebe um SMS, WhatsApp ou e-mail com um link de pagamento falso ou um boleto falso de uma conta legítima.

SITE OU ANÚNCIO FALSO

O consumidor recebe por mensagens, vê nas redes sociais ou em páginas falsas de e-commerce anúncios de promoções ou ofertas fake.

FRAUDE COM CARTÃO DE CRÉDITO

Na hora de pagar a conta, golpistas disfarçados de vendedores prestam atenção na senha digitada e trocam o cartão. Depois usam os dados para compras.

FALSA TAXA DE ENTREGA

A vítima recebe um telefonema ou mensagem dizendo que tem uma entrega a receber e precisa pagar uma taxa. Golpistas usam máquina fraudada e cobram valor mais alto – ou roubam os dados.

GOLPE DA MÃO FANTASMA

Criminoso entra em contato se passando por funcionário do banco, dizendo que a conta foi invadida ou que há movimentações suspeitas. Depois pede que se clique num link para solucionar o problema.

MENSAGEM PEDINDO PIX

Criminoso usa foto de familiar e depois envia mensagem para os contatos dizendo que mudou de número e pede dinheiro por PIX.

HACKEAMENTO DE REDES SOCIAIS

O golpista consegue hackear e “sequestrar” a conta de rede social. A partir daí, faz postagens oferecendo produtos ou oportunidades de investimentos aos amigos da vítima.

ACESSO À CONTA COM ROUBO DO CELULAR

9,3% dos brasileiros reportaram roubo do celular no último ano: o principal objetivo é usar o aparelho para entrar nas contas bancárias das vítimas.

GOLPE DO WHATSAPP

Golpista descobre o número do celular da vítima que quer clonar. Fingindo ser de algum serviço de atendimento ao cliente, pergunta qual foi o código enviado para o aparelho. Com essa informação, consegue concluir a clonagem.

PHISHING

Vítima recebe mensagem por telefone ou e-mail induzindo-a a clicar em links suspeitos ou páginas falsas, e acaba fornecendo dados pessoais.

FALSA CENTRAL TELEFÔNICA

Fraudador entra em contato se passando por funcionário do banco ou empresa, informa que há uma irregularidade na movimentação e solicita dados pessoais.

INVESTIMENTO FALSO

Oferta de investimento com rendimento muito maior do que o oferecido pelos bancos. Muitas vezes o investimento é em criptomoedas e em aplicativos falsos.

FALSO EMPRÉSTIMO

Usando dados do cliente, golpistas fazem um empréstimo em alguma instituição. Depois, entram em contato com o cliente e pedem que faça um Pix de valor específico para que cancelem a operação.

FALSO MOTOBOY

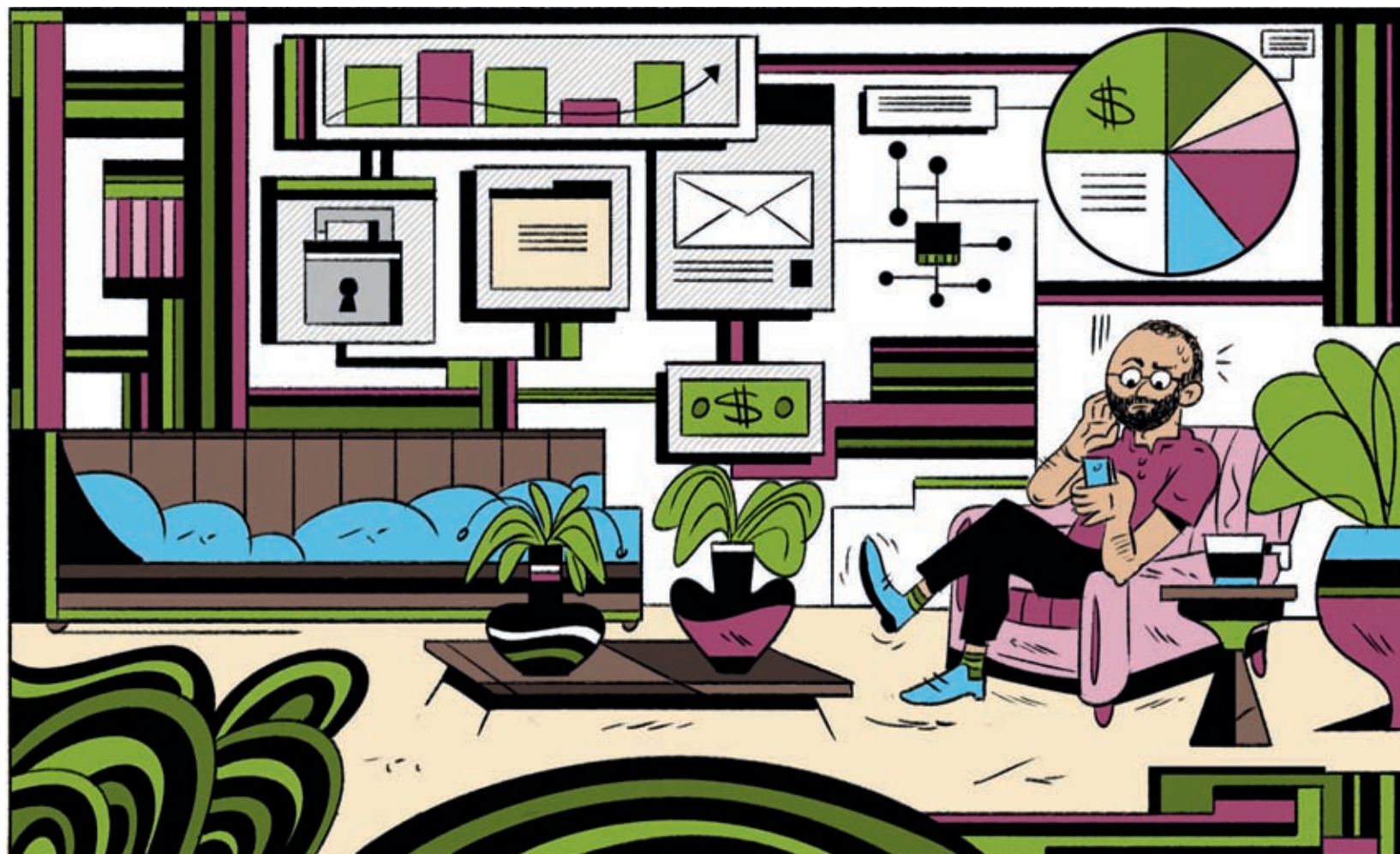
Golpista liga se passando por funcionário do banco e informa que o cartão foi clonado e que é preciso bloqueá-lo. Pede que o cliente digite a senha. Depois, diz que um motoboy vai buscar o cartão para uma perícia.

Essa também é a avaliação do diretor da Equipe Global de Pesquisa e Análise da Kaspersky para a América Latina, Fabio Assolini. Ele afirma que boa parte da prevenção consiste em desconfiar. “O brasileiro gosta de novidades, mas falta educação digital, o que dificulta diferenciar uma mensagem verdadeira de uma falsa”, diz. Somente no ano passado, a Kaspersky bloqueou 309 milhões de tentativas de ataques, uma média de 588 bloqueios por minuto. É verdade, porém, que o maior conhecimento sobre as fraudes vem provocando mudanças no comportamento do consumidor brasileiro. A pesquisa Relatório de Identidade Digital e Fraude, da Serasa Experian, mostra que a segurança é o atributo mais valorizado em compras e atividades online. O modo de pagamento também vem mudando, com aumento do cartão de crédito em detrimento do Pix. O medo dos golpes digitais também transformou o modo de usar o celular em público. A Pesquisa de Vitimização e Percepção sobre Violência e Segurança Pública no Brasil, realizada pelo Datafolha, mostra que 81,6%

dos entrevistados têm aplicativos de banco instalados no smartphone, mas 29,7% têm dois aparelhos e deixam em casa o celular com os apps.

VÍTIMA DO PIX

No mundo, 67% das pessoas acreditam ser capazes de perceber quando estão sendo vítimas de golpes. Mas a verdade é que muitas delas caem nas armadilhas, por conta de vulnerabilidades, da emoção do momento ou da habilidade dos criminosos. Nem todo o conhecimento técnico como empreendedor na área de TI livrou Fernando Seguin, 37 anos, de ser vítima de um golpe do Pix no ano passado. Ele estava a caminho de um jantar quando recebeu uma mensagem de WhatsApp de uma tia que havia visitado recentemente – e que estava numa situação financeira difícil. Ela pedia um empréstimo de R\$ 1,5 mil e dizia que era urgente. Ainda no trânsito, Seguin fez o Pix e enviou o comprovante à tia. Quando recebeu de volta uma resposta automatizada, achou muito estranho. Fez então o que



APOSTA EM CRIPTOMOEDAS Adilson Lima entrou em um grupo do WhatsApp com dicas de investimentos e acabou perdendo R\$ 60 mil

O PASSO A PASSO DA PREVENÇÃO

MUITOS GOLPES DEPENDEM DE UMA AÇÃO DO USUÁRIO PARA SE CONCRETIZAR. DESCONFIE SEMPRE



Nunca passe seus dados em ligações supostamente feitas por bancos ou empresas com as quais você tem uma relação comercial. Na dúvida, ligue para o banco ou empresa pelos canais oficiais.



Nunca clique em links enviados por mensagens para confirmar dados. Pode ser a porta de entrada para programas maliciosos.



Proteja todos os seus equipamentos, em casa e no trabalho, com antivírus atualizado e proteção contra malware.



Não faça fotos com entregadores, ou envie fotos suas para confirmar seus dados. A foto do rosto pode ser usada para abrir contas com biometria facial.



Se uma oferta parece boa demais, um investimento muito lucrativo ou uma promoção imperdível, evite. Não tome decisões por impulso.



Não acredite nem mesmo em mensagens de empresas com selos verificados. Em algumas redes, basta pagar para ter esse selo.



Em nenhuma circunstância baixe arquivos ou instale aplicativos recebidos por e-mail ou mensagens.

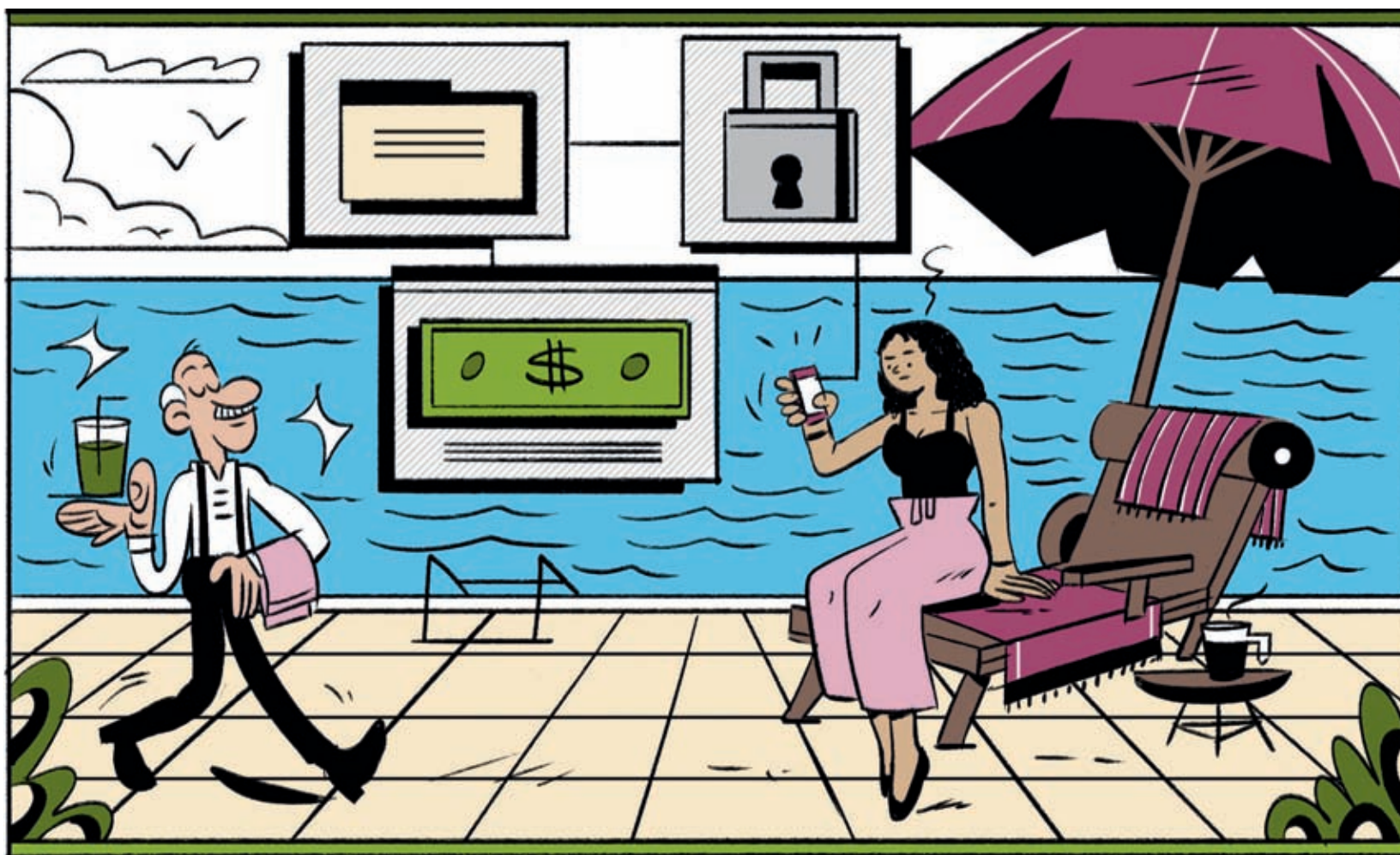


Verifique com frequência se seus dados foram usados para abrir uma conta, criar uma chave PIX ou pedir empréstimo consultando o site Registrato, do Banco Central.



Antes de abrir links enviados por e-mail ou mensagem, verifique se a URL corresponde exatamente ao nome da loja. Sites falsos costumam ter palavras adicionais ou escritas de forma incorreta.

Fontes: Kaspersky, Serasa Experian, Febraban, Procon e DEIC



ROUBO NO CARTÃO Depois de uma ligação falsa do banco, Jamile Lima Pio percebeu uma retirada de R\$ 5 mil com seu cartão de crédito

deveria ter feito antes: ligou para a mãe e perguntou se o WhatsApp da tia havia sido clonado – e a resposta foi positiva. No dia seguinte, entrou em contato com o seu banco e com a instituição para a qual havia enviado o dinheiro e pediu acesso ao MED – Mecanismo Especial de Devolução do Pix, que pode ser acionado quando o cliente é vítima de fraude. Conseguiu reaver parte do dinheiro, mas sua irmã, que sofreu o mesmo golpe, não conseguiu nada de volta. “Esse tipo de fraude pega a gente no emocional”, diz o empreendedor. “Não tem a ver com o seu conhecimento, e sim com o momento que está vivendo.”

Em outro golpe bastante comum, o cliente recebe uma ligação de um número igual ao do seu banco, pedindo para confirmar algumas operações suspeitas. Ao ouvir que você não reconhece as operações, o golpista diz que é preciso instalar um programa para confirmar o cancelamento – e, dessa maneira, consegue a senha da conta. Em algumas situações, diz que vai enviar um entregador para retirar o cartão. A consultora de RH Jamile Lima Pio recebeu

uma ligação dessas em novembro do ano passado, quando estava viajando de férias. A pessoa disse que trabalhava no banco em que ela tinha conta e chegou a mencionar o seu saldo. Depois da conversa, percebeu que havia uma retirada no cartão no valor de R\$ 5 mil, com opção por pagamento parcelado. Ela abriu um boletim de ocorrência e tentou o MED, mas o banco negou e cobrou a dívida. Foi obrigada a pagar quatro parcelas de R\$ 2.119,12. Depois disso, bloqueou todas as ligações e só atende números conhecidos. Além disso, só sai de casa com um cartão e mantém o limite bem baixo. “Como perdi muito dinheiro, fiquei bem mais desconfiada”, afirma.

CRIME ORGANIZADO

Muitos celulares são roubados por quadrilhas especializadas em quebrar senhas, entrar em e-mails e aplicativos bancários e transferir recursos antes mesmo que o consumidor tenha tempo de bloquear as contas. O consultor Dilson Canovas Campos, de 48 anos, conferiu em primeira mão o

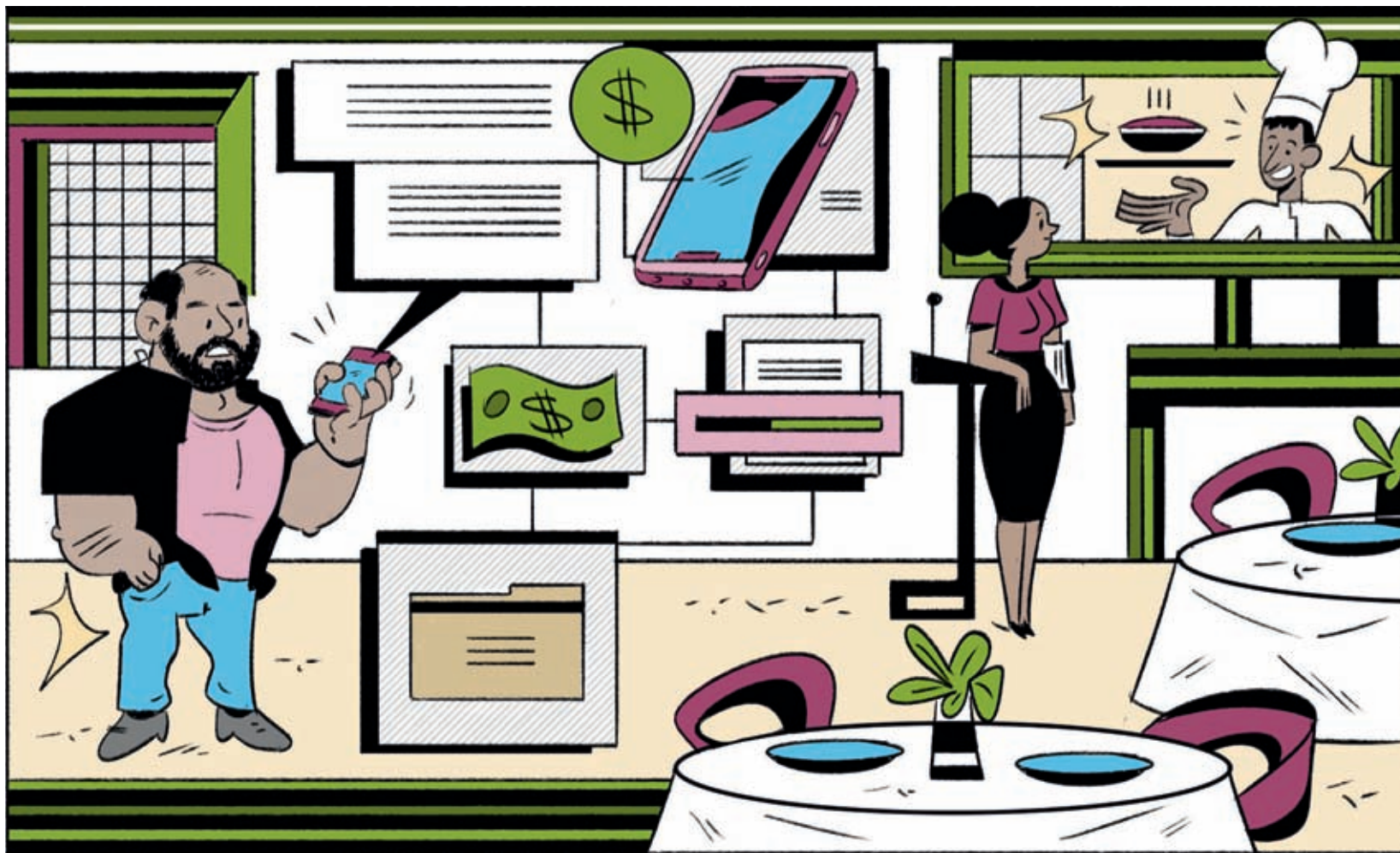
que os criminosos podem fazer quando colocam as mãos em celulares com aplicativos de banco instalados e e-mail desbloqueado. Abordado por dois motoqueiros armados num bairro em São Paulo, ele foi obrigado a entregar dois iPhones desbloqueados, pessoal e do trabalho. “Foi tudo muito rápido. Na moto eles já tinham um equipamento para fazer as transações”, afirma.

Os bandidos mudaram rapidamente a senha do iCloud e ele só conseguiu resolver quando foi pessoalmente à loja da operadora. A essa altura, o prejuízo já somava R\$ 7,3 mil. “Eles pegaram todas as fragilidades do sistema e o exploraram ao máximo”, conta. Agora, Dilson deixa os aplicativos instalados num iPad, que não sai de casa. O telefone que ele usa na rua não tem Pix ou carteira digital. Pagamentos, só com o cartão de crédito físico. “A modernidade você combate com disquete”, brinca ele. “Quando vejo alguém com dois iPhones eu já falo: use dois Apple ID diferentes, mantenha tudo separado. Não existe um tutorial de segurança. Você tem que inventar o seu.”

Falsas entregas de lojas também se tornaram comuns no dia a dia dos brasileiros. O gerente de projetos de TI Laerte Souza da Silva, 38 anos, sofreu um golpe pelo cartão de crédito envolvendo uma falsa entrega. Em setembro do ano passado, no seu aniversário, um golpista ligou para sua esposa, Yngrid Carneiro, dizendo ser de uma floricultura conhecida e informando que sua irmã havia comprado flores para ela, mas deixado o endereço errado. Disse que entregaria no local certo, cobrando uma taxa de R\$ 3, a ser paga no cartão de débito ao entregador. Ela concordou e deu o endereço. Quando o entregador chegou, o cartão não funcionou. Laerte então passou o cartão dele, que também não funcionou. O entregador disse que iria buscar outro equipamento. Foi quando o casal recebeu as notificações: R\$ 600 no cartão de Yngrid e R\$ 3,2 mil no de Laerte. Pensando que o golpe era do entregador, ligaram para o telefone da suposta floricultura, que pediu os dados do cartão, para verificar. Foi quando perceberam que era tudo parte da



FALSO EMPREGO Ana Paula Regiani acreditou que teria que pagar por uma certificação para concorrer a uma vaga e perdeu R\$ 700



EMPRÉSTIMO Fernando Seguin acreditou que estava ajudando uma tia em dificuldades quando fez uma transferência de R\$ 1,5 mil

mesma fraude. “Nós praticamente entregamos o dinheiro na mão deles”, diz Laerte.

Há ainda quem explore o desemprego alheio. Os criminosos anunciam uma determinada vaga e, quando o candidato é selecionado, pedem pagamento para certificações ou outros requisitos. Foi o que aconteceu com a psicóloga clínica Ana Paula Reggiani, 42 anos, de Curitiba. Ela recebeu uma mensagem pelo WhatsApp oferecendo um emprego em um hospital. A condição era que tivesse duas certificações técnicas. A recrutadora indicou uma empresa que faria os documentos. Ela entrou em contato: a foto do WhatsApp parecia ser de uma pessoa que dava cursos na área. Ana Paula pagou R\$ 700 via Pix. Só mais tarde, ao checar suas mensagens, encontrou um e-mail do mesmo hospital, informando que não cobravam por processo seletivo. Foi quando percebeu o golpe, mas o valor já tinha saído da sua conta. “Eu nunca tinha passado por uma situação dessas. Naquele dia estava trabalhando e acabei caindo. Aprendi da pior forma.”

INSTAGRAM ROUBADO

Quem já teve sua rede social hackeada sabe o prejuízo que isso pode causar. Nesses casos, o golpista aproveita o prestígio social e a rede de contatos da vítima para fazer postagens oferecendo produtos para compra ou oportunidades de investimento. Foi o que aconteceu com o professor universitário Pedro Varoni, 62 anos, de São Carlos (SP). Em abril, ele começou a receber mensagens de amigos avisando sobre postagens estranhas no Instagram, que ofereciam dicas de investimentos. Apesar de apelar várias vezes à plataforma, ele só conseguiu recuperar o acesso à sua própria conta três semanas depois, e só com decisão judicial. Em junho, ele ganhou na Justiça uma indenização de R\$ 5 mil pelo transtorno. “Foi uma experiência horrível. É como se você tivesse a sua casa roubada e, para conseguir entrar, tivesse que provar que não é o ladrão”, diz. “Felizmente, meus amigos perceberam que era golpe, pelo tipo de linguagem, e não caíram na armadilha.” **N**