Bolsas — Na sexta-feira: 0,88% São Paulo; 0,77% Nova York

Pontuação B3 — Ibovespa nos últimos dias: 127.528 / 127.027 (19/3, 20/3, 21/3, 22/3)

Dólar — Na sexta-feira: R$ 4,998 (+ 0,39%)

Últimos	
18/março	5,025
19/março	5,029
20/março	4,974
21/março	4,979

Salário mínimo — R$ 1.412

Euro — Comercial, venda na sexta-feira: R$ 5,401

CDI — Ao ano: 10,65%

CDB — Prefixado 30 dias (ao ano): 10,65%

Inflação — IPCA do IBGE (em %)

Outubro/2023	0,24
Novembro/2023	0,28
Dezembro/2023	0,56
Janeiro/2024	0,42
Fevereiro/2024	0,83

SEGURANÇA

Crimes cibernéticos avançam no Brasil

País ocupa a vice-liderança em ranking global de casos, e especialistas alertam sobre os golpes mais frequentes na internet

» RAFAELA GONÇALVES

O Brasil é o segundo país que mais sofre crimes cibernéticos na América Latina. Conforme dados de pesquisa realizada pela SAS Institute, empresa de business intelligence, a maioria dos consumidores brasileiros (80%) disse ter sofrido algum tipo de fraude digital ao menos uma vez, e os dados pessoais e financeiros dos usuários valem ouro para os cibercriminosos.

Com a tecnologia ganhando cada vez mais espaço na vida dos consumidores, quadrilhas tentam tirar proveito por meio de compras on-line, falsas centrais de atendimento e até promessas de renda extra. "Pessoas que antes não utilizavam serviços digitais passaram a utilizar, com isso o acesso aos dados aumenta e acaba abrindo margem para essa ocorrência de golpes e de fraudes. Numa cadeia onde a gente pensa em segurança da informação, o elo mais fraco é sempre o usuário, que às vezes abre brecha para a atuação de quadrilhas especializadas", afirma Neyanne Araújo, advogada especializada em direito digital.

Poucos dias após a liberação da declaração do Imposto de Renda 2024, criminosos já estão aplicando golpes digitais nos contribuintes que querem acertar as contas com o Leão. Segundo o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), foram identificadas campanhas induzindo usuários a baixar e instalar aplicativos falsos a partir das diferentes lojas, como a Google Play Store para dispositivos Android ou Apple Store para dispositivos iOS.

As ferramentas, que imitam o visual e o funcionamento do serviço do Imposto de Renda de Pessoa Física (IRPF) para o ano-base de 2023, visam roubar dados pessoais e financeiros de vítimas, que são levadas a acreditar que estão preenchendo uma declaração de verdade. Esses aplicativos são habilmente promovidos por meio de redes sociais, e-mails enganosos e até mesmo nos resultados de pesquisas on-line, apresentando-se como alternativas confiáveis.

"No período de declaração do Imposto de Renda, muitos brasileiros buscam soluções práticas para cumprir essa obrigação fiscal. É neste momento que os golpistas entram em ação, criando aplicativos fraudulentos que se passam por ferramentas legítimas de auxílio na declaração", destaca Guilherme Guidi, especialista em direito digital do escritório Freitas Ferraz Advogados.

Roubos

De acordo com ele, muitas vezes, os aplicativos estão, inclusive, em lojas oficiais do Android e do iOS, o que dificulta ainda mais a identificação da fraude. "Ao baixá-los, o contribuinte acaba entregando informações preciosas nas mãos de criminosos, que podem usar esses dados para realizar uma série de fraudes financeiras, roubos de identidade ou outras ações criminosas como sequestro, roubo, extorsão, entre outros", alerta o especialista.

As quadrilhas especializadas em cibercrimes estão sempre à espreita de dados pessoais e financeiros. "Nesse caso específico do Imposto de Renda, o problema é potencializado, pois essa declaração feita pelo contribuinte contém geralmente informações detalhadas sobre seus bens, recebimentos e patrimônio, mas pode também indicar muitas outras informações sobre sua vida privada, aumentando ainda mais o risco para as vítimas", explica Guidi.

Um link para um site falso de ingressos para os shows de Caetano Veloso e Maria Bethânia, permaneceu por horas exibido na primeira página de buscas do Google na última semana. A plataforma dos golpistas simulou o ambiente do site oficial, com sistema de fila de espera e diversos detalhes que tornaram muito mais difícil a percepção de que seria um golpe.

A psicóloga Júlia Carvalho, de 32 anos, foi uma das fãs surpreendidas pela fraude. "O site era idêntico, é impressionante. Quando pesquisei no Google a abertura das vendas dos ingressos, foi o primeiro sugerido e era a mesma interface da plataforma real, que estava vendendo os ingressos", conta Júlia, que só se deu conta de que se tratava de um golpe na hora de finalizar o pagamento.

"Eu preenchi todos os meus dados e estranhei porque no pagamento só tinha a opção de pagar por PIX, foi aí que eu me dei conta de que se tratava de um site falso e não fiz o pagamento, só que eu concedi ali todos os meus dados pessoais e não sei o que pode ser feito com eles. É uma sensação horrível passar por esse tipo de situação, por mais que eu não tenha tido a perda financeira no momento, eu não sei o que fazer em relação às informações que preenchi", afirma.

Atenção nas transações

Com os golpes financeiros se tornando cada vez mais comuns, é importante reconhecer os tipos de fraude e manter a atenção nas transações on-line. O advogado Mozar Carvalho, sócio-fundador do escritório Machado de Carvalho Advocacia, diz que os crimes que envolvem o roubo de dados não são uma novidade e que os criminosos apenas aguardam oportunidades para lançar novas ferramentas. "Por trás dessas quadrilhas existem técnicas avançadíssimas para evitar rastreamento e aumentar a eficácia de seus ataques", explica.

A maior recomendação é sempre procurar canais oficiais e é preciso ter cautela para passar longe das armadilhas virtuais: "Recebeu qualquer coisa por e-mail e não sabe de quem é, apague. Muitas vezes, é melhor apagar e perder alguma informação duvidosa do que ficar com a vida enrolada por um bom tempo. Além disso, mantenha nos seus aparelhos softwares de segurança atualizados para você ter uma boa segurança e evitar golpes. Posso garantir que eles geram uma dor de cabeça fora do comum."

O especialista ressalta que, caso você seja a vítima de um golpe, é crucial agir imediatamente. "É preciso notificar os bancos para prevenir fraudes, mude também todas as senhas dos seus dispositivos, para caso o golpe envolva algum tipo de cavalo de troia. Além disso, é indispensável registrar um boletim de ocorrência, que também pode ser feito virtualmente", aconselha Mozar Carvalho.

Aumento da demanda

Quase seis em cada 10 empresas brasileiras sofreram ataques ou incidentes cibernéticos que impediram o acesso aos seus dados em 2023, de acordo com o Índice Global de Proteção de Dados (GDPI). Em resposta a esses desafios, as empresas têm buscado proteção no mercado de seguros.

Esse cenário causou um aumento da demanda por seguros por parte das empresas. Um levantamento da Confederação Nacional das Seguradoras (CNSeg) revela que a procura pelo seguro de Riscos Cibernéticos cresceu 880% nos últimos cinco anos, passando dos R$ 20,7 milhões arrecadados em 2019 para R$ 203,3 milhões em 2023. Em comparação, exclusivamente com o ano de 2022, o avanço foi de 17,1%.

Destinado às empresas, o seguro de Riscos Cibernéticos oferece proteção contra danos diretos ocasionados por ataques que geram perdas materiais, imateriais e de conteúdo informacional, como vazamento de dados. Além disso, pode ser utilizado para cobrir reclamações decorrentes de uso indevido de informações e violação da privacidade e dos direitos de propriedade intelectual.

Segundo a Chain Analysis, empresa americana de análise de blockchain, grupos de hackers captaram US$ 1,1 bilhão com ataques ransomware em 2023 — valor recorde para esse tipo de crime e quase o dobro do prejuízo causado em 2022 (US$ 567 milhões).

A inteligência artificial generativa é uma tecnologia capaz de gerar conteúdo após ser treinada com padrões complexos a partir de uma base de dados. No Brasil, o estudo do GDPI mostrou que a constante jornada de proteção de dados continua sendo um desafio enorme dentro das organizações, sendo quase unânime a percepção dos executivos sobre o aumento da superfície de risco por conta da rápida adoção da IA generativa dentro das empresas, que demandará novas medidas para proteger os dados.

Cerca de 85% dos executivos brasileiros ouvidos acreditam que os dados utilizados para a IA generativa serão altamente distribuídos, aumentando, portanto, a preocupação sobre se estão adequadamente protegidos.

IA para prevenção

À medida que os fraudadores usam, cada vez mais, a tecnologia para enganar consumidores e empresas, o setor financeiro está adotando técnicas de inteligência artificial (IA) generativa para aprimorar proteções. Ao mesmo passo que o avanço da tecnologia é visto como uma ameaça, ele também é a chave para aumentar as camadas de segurança e dificultar os golpes digitais.

Durante a 17ª edição do Congresso de Meios Eletrônicos de Pagamento (CMEP), realizado pela Associação Brasileira das Empresas de Cartões de Crédito e Serviços (Abecs), foram debatidas as perspectivas para segurança e digitalização. Para Fernando Amaral, vice-presidente de inovação e soluções da Visa do Brasil, o uso de dados dos clientes e a IA têm que andar juntos para aprimorar a segurança nas transações financeiras.

"O avanço da quantidade de dados e você compartilhar dentro do ecossistema cuidadosamente vai ajudar muito na segurança e aplicar modelos de inteligência artificial nessas soluções vão garantir cada vez mais proteção, para evitar esses transtornos que acontecem no dia a dia das pessoas", afirma Amaral.

A multinacional de serviços financeiros lançou recentemente o Visa Secure Data Only (VSDO), desenvolvido com o objetivo de simplificar a troca de dados entre emissores e estabelecimentos comerciais. "Essa ferramenta permite que o comércio compartilhe em tempo real dados que fazem com que o emissor tenha mais segurança para fazer uma transação, para garantir que você é você mesmo", explica o vice-presidente de inovação.

Outra ferramenta aprimorada para a segurança das transações on-line no Brasil é o Click to Pay, uma nova opção de pagamento digital para o e-commerce. Em fevereiro deste ano, a Mastercard habilitou as primeiras operações por meio do sistema que usa a tecnologia de tokenização. "A informação que trafega durante a transação substitui aquele número de 16 dígitos que tem no seu cartão, um token faz o uso de uma combinação exclusiva de números que é usada apenas para aquela transação. Mesmo se eventualmente tivesse algum tipo de fraude, esses dados não serviriam para absolutamente nada", destaca Marcelo Tangioni, presidente da Mastercard Brasil.

A tecnologia se trata da combinação entre agilidade, com a redução de cliques na hora da compra, e camadas de proteção ao consumidor. "Tudo que fazemos na indústria de meios de pagamentos tem que estar pautado por dois temas, praticidade e segurança. Estamos lidando com dinheiro das pessoas e de estabelecimentos comerciais, então a segurança é fundamental", reforça Marcelo Tangioni. **(RG)**

Internautas na mira

Conheça os golpes financeiros mais aplicados nos meios digitais e saiba como se proteger

Phishing

- No phishing, os criminosos criam anúncios, enviam e-mails ou mensagens de texto falsas que parecem ser de uma empresa legítima para obter informações pessoais ou financeiras do usuário.
- Eles podem pedir ao usuário para clicar em um link malicioso ou baixar um anexo infectado com "malware", que é uma espécie de sistema utilizado para espionar as atividades feitas no celular e computador e roubar os dados.
- Os usuários devem sempre verificar cuidadosamente o remetente do e-mail ou mensagem de texto e evitar clicar em links suspeitos ou baixar anexos de remetentes desconhecidos.

Pharming

- Esta técnica envolve o sequestro do computador do usuário para redirecioná-lo para um site falso, mesmo que o usuário tente acessar o site real.
- Os criminosos podem usar "malware" para infectar o computador sem que o usuário tenha conhecimento do que está acontecendo.
- Os usuários devem manter seus sistemas operacionais e software de segurança atualizados e usar um antivírus confiável para proteger seus computadores.
- Também é importante verificar cuidadosamente o URL do site que estão visitando e evitar clicar em links suspeitos ou baixar anexos de remetentes desconhecidos.

Golpe da renda extra

- A promessa de dinheiro extra para as vítimas curtirem fotos em redes sociais ou avaliar produtos em sites. O importante para se proteger desse golpe é desconfiar de promessas infundadas do "dinheiro fácil", que em sua maioria, são falsas.

Fraude de antecipação de recursos

- Nesse golpe, criminosos exigem pagamentos antecipados por produtos ou serviços inexistentes, utilizando sites falsos ou anúncios enganosos.
- Um exemplo é o golpe do empréstimo consignado, onde os criminosos oferecem liberar o consignado facilmente para quem está negativado e pedem o pagamento antecipado de taxas, afirmando que é uma prática dentro da lei.
- Para evitar essa fraude, é fundamental verificar a reputação do vendedor e contratar o crédito com empresas que já são conhecidas no mercado.

Golpe da falsa central

- Por meio de um falso SMS ou ligação fingindo ser a central de atendimento do seu banco, o criminoso indica que houve alguma fraude em seu cartão de crédito para fazer com que a vítima passe informações confidenciais.
- Para prevenção a esse golpe, é indicado que sempre cheque com os números oficiais do banco se de fato houve alguma fraude com seu cartão.

Roubo de dados

- Os criminosos podem roubar informações pessoais por meio de "phishing", "malware" ou outras técnicas de engenharia social. Ao fornecer dados pessoais, você está se sujeitando a ter suas informações vazadas ou utilizadas para outros golpes, como clonagem de WhatsApp e de cartões.
- Os criminosos também podem usar essas informações para abrir contas em nome da vítima, solicitar empréstimos ou cometer outros crimes financeiros. Os usuários devem ter cuidado ao compartilhar informações pessoais on-line e proteger suas contas com senhas fortes e autenticação de dois fatores sempre que possível.

Valdo Virgo/CB/D.A Press

Fonte: Eset.