OPINIÃO

Proteja seu mundo com Passkeys, as chaves de acesso resistentes a phishing

Sérgio Muniz (*)

Ao celebrarmos o Mês de Conscientização sobre Segurança Cibernética de 2024 com o tema "Proteja Nosso Mundo", explorar tecnologias inovadoras é crucial para nos ajudar a atingir essa meta.

Um desses avanços que está revolucionando a segurança online e a autenticação do usuário são as passkeys. Essas chaves de acesso representam um salto significativo na criação de um cenário digital mais seguro, alinhando-se perfeitamente com a missão de proteger nosso mundo. Ao alavancar técnicas criptográficas e autenticação biométrica, as chaves de acesso oferecem uma alternativa mais robusta e amigável às senhas tradicionais, abordando muitas vulnerabilidades que há muito tempo atormentam nossas contas online.

Neste artigo, vamos nos aprofundar em como as passkeys funcionam, seus benefícios e por que elas são uma ferramenta essencial em nosso esforço coletivo para construir um futuro digital mais seguro para todos.

Phishing, uma epidemia crescente

O phishing é eficaz porque capitaliza a psicologia humana, explorando viés e comportamentos naturais em vez de mirar em fraquezas tecnológicas. Também é popular porque uma tentativa bem sucedida de phishing pode dar aos criminosos uma posição nas redes empresariais, levando a violações de dados e perdas financeiras.

Apesar dos esforços contínuos para aumentar a conscientização, esses ataques exploram com sucesso nossos vieses e preconceitos para contornar os sistemas de segurança tradicionais baseados em senhas. Eles convencem as pessoas a fornecer informações confidenciais, como senhas ou logins, disfarçando-se de entidades confiáveis, tornando as senhas o elo mais fraco na cadeia de segurança cibernética. Vejamos algumas estatísticas:

- No primeiro trimestre de 2024, mais de 963 mil sites exclusivos de phishing foram detectados globalmente.
- Em 2023, o IC3 recebeu um número recorde de reclamações de pessoas nos EUA, totalizando 880.418 reclamações com perdas potenciais superiores a US$ 12,5 bilhões.
- O Relatório Global de Ameaças a Dados da Thales de 2024 revelou que o erro humano continua sendo a principal causa de violações de dados, com 31% das empresas identificando isso como a causa raiz.

Não é nenhuma surpresa que o Mês de Conscientização sobre Segurança Cibernética deste ano incentive a todos nós cidadãos a ficarmos vigilantes sobre phishing. A educação tem um papel a desempenhar aqui, mas adotar mecanismos de autenticação mais fortes e resistentes a phishing, como as passkeys, pode ser ainda mais eficaz na prevenção desse flagelo.

Como funcionam as passkeys?

As passkeys foram projetadas para eliminar as fraquezas inerentes às senhas. Elas fornecem logins mais rápidos, fáceis e seguros para sites e aplicativos e são resistentes a phishing.

Elas são baseadas no padrão Fast Identity Online (FIDO), com um par de chaves criptográficas (chaves pública e privada) que autentica usuários sem colocar dados confidenciais (como senhas) em risco de esquemas de phishing. Na verdade, elas eliminam completamente a necessidade de senhas.

Ao contrário das senhas, que podem ser facilmente roubadas ou vítimas de phishing, as passkeys nunca saem do dispositivo do usuário e não podem ser interceptadas por malfeitores. Elas são um salto gigante em direção à autenticação sem senha, aumentando a segurança em entidades do setor público e privado.

As passkeys também aprimoram a autenticação multifator (MFA). A MFA precisa que os usuários forneçam dois ou mais formulários de verificação; as passkeys simplificam o processo integrando dados biométricos ou um PIN com autenticação criptográfica.

Tipos de Passkeys: sincronizadas e vinculadas ao dispositivo

Existem dois tipos de Pass Keys: sincronizadas e passkeys vinculadas ao dispositivo. Embora ambas ofereçam resistência a phishing, elas funcionam de forma diferente em termos de segurança e experiência do usuário.

Passkeys sincronizadas: elas são armazenadas na nuvem e podem ser sincronizadas em vários dispositivos. Gigantes da tecnologia como Apple, Google e Microsoft usam passkeys sincronizadas para melhorar a experiência do usuário. Elas podem ser facilmente transferidas entre dispositivos para que os usuários possam fazer login com um PIN ou uma biometria (impressão digital ou reconhecimento facial). Elas são convenientes para uso pessoal, permitindo que os usuários acessem contas de diferentes dispositivos sem atrito.

Passkeys vinculadas ao dispositivo: elas são vinculadas a um dispositivo específico e nunca o deixam. Isso as torna mais seguras do que chaves de acesso sincronizadas, pois a chave privada permanece protegida contra ameaças externas, como ataques na nuvem. Às vezes, elas vêm na forma de chaves de segurança de hardware, como tokens USB ou cartões inteligentes, que exigem a posse física do dispositivo para autenticação. As passkeys vinculadas ao dispositivo são particularmente úteis para empresas com altos requisitos de segurança, pois fornecem uma camada extra de proteção contra ataques de phishing e man-in-the-middle.

Qual é a Passkey certa para o seu negócio?

A Passkey sincronizada é conveniente para contas pessoais e uso diário, e a Passkey vinculada ao dispositivo é a opção mais adequada para empresas que priorizam a segurança. As empresas que lidam com dados confidenciais ou aquelas sujeitas a requisitos de conformidade rigorosos devem optar por passkeys vinculadas ao dispositivo para evitar phishing, ataques man-in-the-middle e outros tipos de roubo de identidade.

Quando a conveniência é a prioridade, as passkeys sincronizadas são ideais para aplicativos ou serviços internos que não lidam com informações críticas.

A pressão por uma autenticação mais forte

À medida que os ataques de phishing se tornam mais sofisticados, governos e reguladores defendem medidas de segurança mais robustas. Na União Europeia, o Regulamento Geral de Proteção de Dados (GDPR) e no Brasil a Lei Geral de Proteção de Dados (LGPD) exigem que as empresas implementem medidas de segurança, que MFA e passkeys abordam de forma abrangente.

Da mesma forma, a Ordem Executiva 14028 direcionou o uso de MFA resistente a phishing nos Estados Unidos, solicitando explicitamente soluções baseadas em FIDO. Esse impulso regulatório fez a demanda por passkeys disparar, principalmente em setores altamente regulamentados que lidam com dados confidenciais, como finanças, saúde e setor público.

Protegendo Nosso Mundo

Na luta para "Proteger Nosso Mundo", as passkeys oferecem uma solução poderosa para uma das ameaças mais difundidas à segurança cibernética: phishing. Ao substituir senhas vulneráveis por autenticação resistente a phishing, as passkeys são o futuro da segurança digital.

Como o Mês de Conscientização sobre Segurança Cibernética nos lembra, reconhecer e relatar phishing é essencial para proteger nosso mundo digital. Ao adotar métodos de autenticação mais fortes, como passkeys, podemos dar um passo adiante na proteção da navegação online e das informações confidenciais.

(*) Vice-presidente de Vendas para Gestão de Identidade e Acesso de Thales para América Latina.

Perigo

Bicicletas podem ser hackeadas

O ciclismo de estrada é um esporte muito popular na Europa; as provas mais conhecidas são Vuelta a España, Tour de France e Giro d'Italia.

Vivaldo José Breternitz (*)

PhonlamaiPhoto_CANVA

Essas competições movimentam muito dinheiro em prêmios, publicidade, apostas etc; por essa razão acabam sendo frequentes as tentativas de fraude, sendo a mais comum o doping dos atletas.

A Internet das Coisas tem trazido benefícios a inúmeras áreas, mas agora pesquisadores afirmam que ela pode ser utilizada para a prática de um novo tipo de fraude nas provas de ciclismo de estrada, pois certos componentes das bicicletas têm vulnerabilidades que permitem ataques remotos durante competições.

Esses pesquisadores, da Northeastern University e da University of California, San Diego, dizem que as bicicletas de hoje são sistemas ciberfísicos que contêm sistemas embarcados que acessam computadores para fins de telemetria e controle, além de apoiarem certas atividades dos ciclistas, especialmente a troca de marchas – esses são os principais pontos que as tornam vulneráveis.

Os pesquisadores concentraram seu trabalho em câmbios fornecidos pela Shimano, uma empresa japonesa que é uma das maiores vendedoras de peças para bicicletas do mundo e concluíram que esses equipamentos são vulneráveis a "replay attacks", como aqueles frequentemente direcionados a chaves de carros.

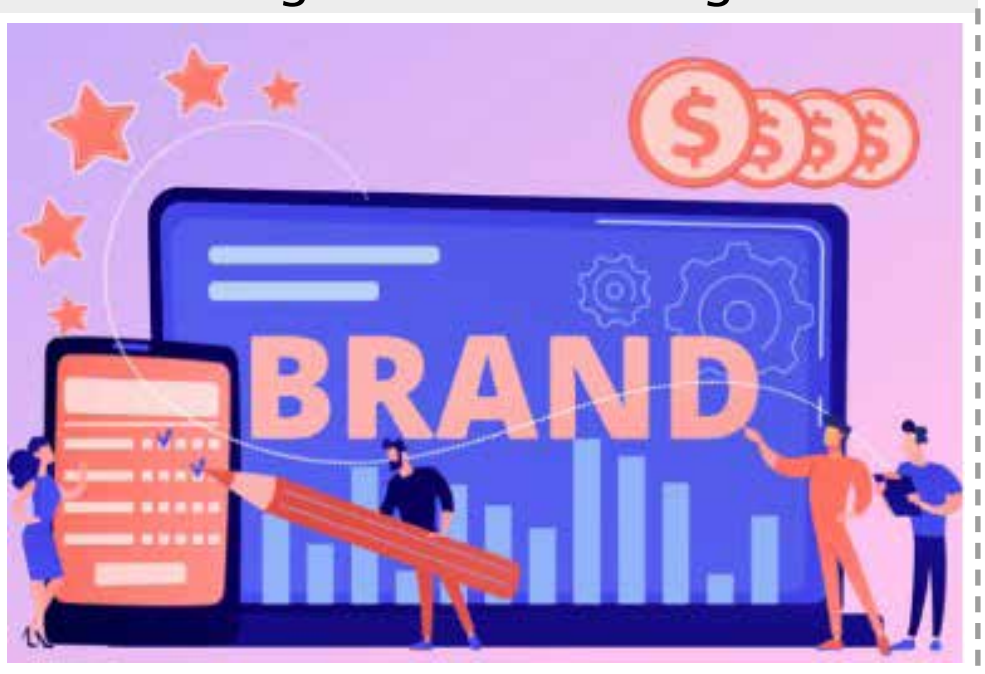
Numa situação de corrida, os atacantes poderiam trocar marchas ou travar o câmbio de algum competidor que pretendessem prejudicar. Além dos prejuízos ao desempenho, poderiam ocorrer também acidentes e lesões graves, dadas as altas velocidades atingidas nessas provas – note-se que o hardware necessário à prática desses ataques é relativamente barato.

A Shimano vive tempos difíceis: além da vulnerabilidade agora tornada pública, no ano passado a empresa foi vítima de um ataque de ransomware e, após se recusar a pagar, teve vários terabytes de seus dados corporativos vazados na internet.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

Cinco motivos para empresas priorizarem a proteção de marca nas estratégias de marketing

Em um mundo cada vez mais competitivo, as empresas precisam adotar uma abordagem abrangente para suas estratégias de marketing. Entretanto, um dos aspectos mais cruciais, muitas vezes negligenciado, é a proteção de marca. Além disso, o assunto se torna ainda mais urgente em meio ao grande número de golpes praticados pela internet, com ajuda de canais, redes e apps digitais.



Por conta disso, Diego Daminelli, CEO da Branddi, empresa especialista no combate à concorrência desleal no ambiente digital, compartilha a seguir cinco motivos pelos quais as empresas e profissionais de marketing devem priorizar essa questão em suas estratégias. Confira:

Preservação da reputação - A reputação de uma marca é um dos ativos mais valiosos de uma empresa. A proteção de marca ajuda a evitar o uso indevido e a apropriação indevida de sua identidade, garantindo que a imagem da marca permaneça intacta. Com a proteção adequada, as empresas podem mitigar riscos de danos à reputação causados por concorrentes desleais ou pela má utilização de suas marcas.

Redução de perdas financeiras - O uso indevido de marcas pode levar a perdas financeiras significativas. Quando uma marca não é protegida, concorrentes podem se beneficiar de sua reputação, prejudicando suas vendas. Investir em proteção de marca é uma forma eficaz de prevenir perda de receita.

Aumento da confiança do consumidor - Marcas bem protegidas transmitem segurança e profissionalismo. Os consumidores tendem a confiar mais em marcas que são reconhecidas e devidamente registradas. Essa confiança se traduz em lealdade, o que é fundamental para o sucesso a longo prazo de qualquer empresa.

Vantagem competitiva - No ambiente de negócios atual, ter uma marca forte e protegida pode oferecer uma vantagem competitiva significativa. Empresas que investem na proteção de suas marcas não apenas se destacam, mas também podem explorar novas oportunidades de mercado, sabendo que sua propriedade intelectual está resguardada.

Cumprimento de normas e regulamentações - A proteção de marca não é apenas uma questão de estratégia de marketing, mas também uma exigência legal em muitos países. As empresas devem garantir que estão em conformidade com as normas e regulamentações relacionadas à propriedade intelectual. A falta de proteção pode resultar em sanções legais, complicações regulatórias e, em última instância, prejuízos financeiros.

"Priorizar a proteção de marca nas estratégias de marketing não é apenas uma boa prática, mas, sim, uma necessidade estratégica que pode impactar diretamente o sucesso e a sustentabilidade de uma empresa. Ao investir na proteção de suas marcas, as empresas não apenas protegem seus ativos, mas também posicionam-se para um crescimento mais robusto e sustentável", ressalta Diego Daminelli, CEO da Branddi.

News @TI

ricardosouza@netjen.com.br

Faculdade Cultura Inglesa oferece cursos gratuitos para Enem 2024

@A Faculdade Cultura Inglesa, instituição de ensino superior com foco na formação e especialização de profissionais da área da língua inglesa, abriu as inscrições para a realização de cursos preparatórios gratuitos para o exame do Enem 2024. Formatados no modelo online assíncrono, com conteúdos gravados, os cursos oferecem insumos para a realização das provas de Inglês, Português e Literatura, que serão aplicadas no dia 03 de novembro. Voltadas para alunos do ensino médio, provenientes de escolas públicas ou privadas, as aulas são ministradas por professores mestres e doutores da instituição (https://www.faculdadeculturainglesa.com.br/extensao-e-cursos-livres/estude-para-o-enem-com-cursos-gratuitos/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.