SEJA CIBERESPERTO
#CyberMonth

MÊS DA CONSCIENTIZAÇÃO EM CIBERSEGURANÇA 2021: FAÇA SUA PARTE. #BECYBERSMART

ROUBO DE IDENTIDADE E GOLPES PELA INTERNET

A tecnologia dos dias de hoje significa que nós podemos nos conectar ao mundo todo, usar o banco e fazer compras on-line e controlar nossos televisores, casas e carros usando um smartphone. Essa praticidade adicional também traz um risco aumentado de roubo de identidade e fraudes pela internet. Seja cibereseperto (#BeCyberSmart) na internet, em casa, na escola, no trabalho, nos dispositivos móveis e na rua.

VOCÊ SABIA?

- Em 2020, o custo médio de uma violação de dados para uma empresa dos EUA foi de US$8,84 milhões[1]. Isso representa um aumento de US$8,64 milhões em relação aos valores de 2019.
- 7-10% da população dos Estados Unidos são vítimas de fraude de identidade a cada ano, e 21% dessas pessoas são afetadas por múltiplos incidentes de fraude de identidade[2].
- Em 2020, 47% das pessoas que moram nos EUA sofreram roubo de identidade[3].

GOLPES COMUNS PELA INTERNET

Conforme a tecnologia continua a evoluir, os cibercriminosos passam a usar técnicas mais sofisticadas para explorar sistemas, contas e dispositivos para roubar sua identidade, informações pessoais e dinheiro. Para se proteger das ameaças on-line, você precisa saber o que procurar. Alguns dos golpes mais comuns na internet são:

- **FRAUDES DE COVID-19,** na forma de e-mails com anexos ou links maliciosos para sites fraudulentos para enganar as vítimas e fazê-las revelar informações sigilosas ou contribuir para instituições de caridade ou causas fraudulentas. Tome cuidado ao lidar com qualquer e-mail com linha de assunto, anexo ou hiperlink relacionados à COVID-19, e desconfie de pedidos em redes sociais, SMS ou telefonemas relacionados à COVID-19.
- **FRAUDES DE IMPOSTORES,** que ocorrem quando você recebe um e-mail ou chamada de uma pessoa que alega ser um funcionário do governo, membro da família ou amigo e pede informações pessoais ou financeiras. Por exemplo, um impostor pode entrar em contato com você como se fosse da Administração de Seguro Social, dizendo que seu número do seguro social (SSN) foi suspenso na esperança de que você revele seu SSN ou pague para reativá-lo.
- **FRAUDES DE PAGAMENTOS ECONÔMICOS RELACIONADOS À COVID-19** estão voltadas para os pagamentos de estímulo para os americanos. A CISA pede a todos os americanos que fiquem alertas para fraude relacionada aos pagamentos devido ao impacto econômico da COVID-19 — especialmente fraude que usa o coronavírus como isca para roubar informações pessoais e financeiras, além dos próprios pagamentos por impacto econômico —, e para adversários que buscam atrapalhar os esforços de pagamento.

DICAS SIMPLES

- **DOBRE SUA PROTEÇÃO DE LOGIN.** Habilite a autenticação multifator (MFA) para garantir que a única pessoa com acesso à sua conta seja você. Use-a para o e-mail, redes sociais e qualquer outro serviço que exija login.

Se houver opção de MFA, habilite-a usando um dispositivo móvel confiável, como seu smartphone, um aplicativo de autenticação ou um token de segurança (um pequeno dispositivo físico que você pode colocar no chaveiro).

- **RENOVE SEU PROTOCOLO DE SENHAS.** Segundo as orientações do Instituto Nacional de Padrões e Tecnologia (NIST), você deve tentar utilizar a senha ou frase secreta mais comprida possível. Use a criatividade e personalize sua senha padrão para sites diferentes, o que pode impedir que os cibercriminosos tenham acesso a essas contas e pode proteger você em caso de violação. Utilize gerenciadores de senhas para gerar senhas diferentes e complexas para cada uma das suas contas e se lembrar delas. Leia Dicas de criação de senha para obter mais informações.
- **MANTENHA TUDO ATUALIZADO.** Mantenha seu software atualizado para a última versão disponível. Faça suas configurações de segurança para manter suas informações seguras, habilitando atualizações automáticas para não precisar pensar nisso, e configure o software de segurança para fazer varreduras regulares.

PROTEJA-SE CONTRA GOLPES ON-LINE

PROTEJA-SE DURANTE A CONEXÃO: A moral da história é que sempre que você estiver on-line, está vulnerável. Se os dispositivos na sua rede estiverem comprometidos por alguma razão, ou se os hackers contornarem um firewall criptografado, alguém pode estar lhe espionando, mesmo na sua própria casa com Wi-Fi criptografado.

- Pratique a navegação segura da web em todos os lugares, procurando o ícone de "cadeado verde" na barra do seu navegador da web; isso indica uma conexão segura.
- Quando você se encontrar no "Wi-Fi selvagem", evite o acesso gratuito à Internet sem criptografia.
- Se você utilizar um ponto de acesso público desprotegido, coloque em prática bons hábitos de internet, evitando atividades sensíveis (como acessar o banco) que exigem senha ou cartões de crédito. Seu hotspot pessoal geralmente é mais seguro que o Wi-Fi gratuito.
- Não revele suas informações de identificação pessoal, como número da conta de banco, SSN ou data de nascimento, para desconhecidos.
- Digite a URL do site diretamente na barra de endereços, em vez de clicar em links ou copiar e colar do e-mail.

RECURSOS DISPONÍVEIS PARA VOCÊ

Se você descobrir que foi vítima de cibercrime, informe imediatamente as autoridades para fazer uma queixa. Mantenha e registre todas as evidências do incidente e sua fonte presumível. A lista abaixo tem as organizações governamentais para as quais você pode fazer uma denúncia se for vítima de cibercrime.

- **FTC.gov**: O recurso completo e gratuito da FTC, www.identitytheft.gov/, pode ajudar você a denunciar e a se recuperar do roubo de identidade. Denuncie golpes à FTC no site ftc.gov/OnGuardOnline ou www.ftccomplaintassistant.gov.
- **US-CERT.gov**: Notifique as vulnerabilidades do computador ou da rede para a US-CERT pela linha direta: 1-888-282-0870 ou us-cert.cisa.gov. Encaminhe e-mails ou sites de phishing para US-CERT no endereço phishing-report@us-cert.gov.
- **IC3.gov**: Se você for vítima de um crime cibernético, faça uma queixa no Centro de Reclamações de Crimes na Internet (IC3), no site www.IC3.gov.
- **SSA.gov**: Se você acha que alguém está usando seu SSN, entre em contato com a linha direta de fraude da Administração de Seguro Social no telefone 1-800-269-0271.

ENTRE EM CONTATO COM A EQUIPE DO MÊS DA CONSCIENTIZAÇÃO EM CIBERSEGURANÇA DA CISA

Agradecemos o seu contínuo apoio e compromisso com o Mês da Conscientização em Cibersegurança e sua ajuda para manter todos os americanos seguros e protegidos on-line. Envie um e-mail para nossa equipe no endereço CyberAwareness@cisa.dhs.gov ou acesse https://www.cisa.gov/cybersecurity-awareness-month ou https://staysafeonline.org/cybersecurity-awareness-month/ para saber mais.

RECURSOS

1. Brook, Chris. (18 de agosto de 2020). *What Does a Data Breach Cost in 2020?* Digital Guardian. https://digitalguardian.com/blog/what-does-data-breach-cost-2020
2. Ricks, A, Irvin-Erickson, Y, PhD (2021). *Research Brief: Identity Theft and Fraud.* Center for Victim Research. https://ncvc.dspacedirect.org/bitstream/item/1228/CVR Research Syntheses_Identity Theft and Fraud_Brief.pdf
3. GIACT. (2021). *U.S. Identity Theft: The Stark Reality*. GIACT Systems, LLC.https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/