SEJA CIBERESPERTO
#CyberMonth

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

PRIVACIDADE ON-LINE

A internet está presente em quase todos os aspectos do nosso cotidiano. Conseguimos fazer compras, usar o banco, conversar com parentes e amigos e gerenciar nossos registros médicos on-line. Essas atividades exigem que você forneça informações de identificação pessoal (PII), como nome, data de nascimento, números de conta, senhas e informações sobre sua localização. Seja ciberesperto (#BeCyberSmart) ao compartilhar informações pessoais on-line para reduzir o risco de se tornar vítima de cibercrime.

VOCÊ SABIA?

- 72% dos americanos acreditam que a maior parte do que fazem on-line está sendo monitorado por anunciantes, firmas de tecnologia e outras empresas.[1]
- Mais da metade dos americanos (52%) disseram ter decidido não usar um produto ou serviço porque estavam preocupados com a quantidade de informações pessoais recolhidas sobre eles.[1]
- O custo das violações de dados aumentou de USD 3,86 milhões para USD 4,24 milhões em 2021.[2]
- Credenciais comprometidas, como senhas, foram responsáveis por 20% das violações, a um custo médio de USD 4,37 milhões por violação.[2]

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). Leia Guia de autenticação multifator (MFA) para saber mais informações.
- **Renove seu protocolo de senhas.** Use a senha ou frase secreta mais longa 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 na 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.
- **Tudo que você conecta deve ser protegido.** A melhor defesa contra vírus e malware, seja para proteger seu computador, smartphone, dispositivo de jogo ou outros dispositivos conectados à rede, é atualizá-los com o mais recente software de segurança, navegador e sistema operacional. Ative as atualizações automáticas, se puder, e proteja seus dispositivos usando um antivírus. Leia Dicas sobre phishing para obter mais informações.

- **Faça-se de difícil com estranhos.** Os cibercriminosos usam táticas de phishing na esperança de enganar suas vítimas. Se você não tiver certeza sobre a origem de um e-mail, mesmo que os detalhes pareçam estar certos, ou se o e-mail parecer suspeito, não responda e não clique em nenhum link ou anexo desse e-mail. Se essas opções estiverem disponíveis, marque como "lixo eletrônico" ou "bloquear" para deixar de receber mensagens de remetentes específicos.
- **Nunca clique para se gabar.** Limite as informações que você posta nas redes sociais, desde endereços pessoais até o local onde você gosta de comprar café. Muitas pessoas não se dão conta de que bastam esses detalhes aparentemente aleatórios para que os criminosos saibam como atingir você, seus entes queridos e seus pertences físicos, tanto on-line quanto no mundo real. Mantenha em segredo números de Seguro Social, números de conta e senhas, além de informações específicas sobre você, como nome completo, endereço, data de aniversário e até mesmo seus planos para as férias. Desabilite serviços de localização que permitem que qualquer pessoa saiba onde você está — ou não — em um dado momento. Leia Dicas de cibersegurança em redes sociais para obter mais informações.
- **Vigie seus aplicativos.** A maioria dos eletrodomésticos, brinquedos e dispositivos conectados são apoiados por um aplicativo móvel. Seu dispositivo móvel pode estar cheio de aplicativos suspeitos rodando em segundo plano ou usando permissões padrão que você aprovou sem se dar conta, recolhendo suas informações pessoais sem o seu conhecimento e colocando sua identidade e privacidade em risco ao mesmo tempo. Verifique as permissões dos seus aplicativos e use a "regra do menor privilégio" para apagar o que não precisa ou não usa mais. Aprenda a dizer "não" para solicitações de privilégio que não fazem sentido. Só baixe aplicativos de fornecedores e fontes confiáveis.
- **Proteja-se durante a conexão.** Antes de se conectar a qualquer hotspot sem fio público — como em um aeroporto, hotel ou café — confirme o nome da rede e os procedimentos exatos de login com o pessoal adequado para se certificar de que a rede é legítima. Se você usar 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. Utilize apenas sites que comecem com "https://" quando fizer compras ou acessar o banco on-line.

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 www.cisa.gov/cybersecurity-awareness-month ou https://staysafeonline.org/cybersecurity-awareness-month/ para saber mais.

RECURSOS

1. Auxier, Brooke, "How Americans see digital privacy issues amid the COVID-19 outbreak." Pew Research Center: Fact Tank. 4 de maio de 2020. https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/
2. IMB, "Cost of a Data Breach Report 2021." IMB Security. Julho de 2021. https://www.ibm.com/security/data-breach