SEJA CIBERESPERTO
#CyberMonth

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

PROTEJA SUA CASA DIGITAL

Hoje em dia a maioria dos dispositivos domésticos está conectada à internet, incluindo termostatos, travas de porta, máquinas de café e alarmes de fumaça. Isso nos permite controlar os dispositivos usando um smartphone, o que pode economizar tempo e dinheiro e oferecer praticidade e até mesmo segurança. Esses avanços da tecnologia são inovadores e intrigantes, mas também trazem novos riscos de segurança. Seja ciberesperto (#BeCyberSmart) para se conectar com segurança e proteger sua casa digital.

DICAS SIMPLES

- **Proteja sua rede Wi-Fi.** O roteador sem fio da sua casa é a principal porta de entrada para que os cibercriminosos acessem todos os seus dispositivos conectados. Troque a senha e o nome de usuário padrão para proteger a rede Wi-Fi e os dispositivos digitais. Para mais informações sobre como proteger sua rede doméstica, consulte a página Proteção de redes sem fio da CISA.
- **Duplique 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.
- **Se você se conecta, deve se proteger.** A melhor defesa contra vírus e malware, seja para proteger seu computador, smartphone, dispositivo de jogo ou outros dispositivos conectados à rede, é se manter em dia e atualizá-los com o mais recente software de segurança, navegador e sistema operacional. Se você tiver a opção de habilitar atualizações automáticas para se defender contra os últimos riscos, faça isso. E, se estiver colocando algo no seu dispositivo, como USB para um disco rígido externo, certifique-se de que o software de segurança do seu dispositivo faça uma varredura em busca de vírus e malware. Por último, proteja seus dispositivos com software antivírus e certifique-se de fazer backups periódicos de todos os dados que não podem ser recriados, como fotos ou documentos pessoais.
- **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.
- **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.

- **Tome cuidado ao usar o compartilhamento de arquivos.** O compartilhamento de arquivos entre dispositivos deve ser desabilitado quando não for necessário. Sempre opte por permitir o compartilhamento de arquivos usando apenas a rede doméstica ou do trabalho, nunca através de redes públicas. Pense também em criar um diretório exclusivo para o compartilhamento de arquivos, restringindo o acesso a todos os outros diretórios. Além disso, você deve proteger com senha tudo o que compartilhar.
- **Verifique as opções de segurança sem fio do seu provedor de internet ou do fabricante do seu roteador.** O provedor de serviços de internet e o fabricante do roteador podem oferecer informações ou recursos para lhe ajudar a proteger sua rede sem fio. Consulte a área de atendimento ao cliente dos respectivos sites para sugestões ou instruções específicas.
- **Conecte-se usando uma rede virtual privada (VPN).** Muitas empresas e organizações têm uma VPN. As VPNs permitem que os funcionários se conectem de forma segura à sua rede quando não estão no escritório. As VPNs criptografam a conexão na saída e na chegada e exclui qualquer tráfego que não esteja adequadamente criptografado. Se você tiver acesso a uma VPN, certifique-se de fazer o login nela sempre que precisar utilizar um ponto de acesso sem fio público.
- **Restrinja o acesso.** Só permita que usuários autorizados acessem sua rede. Cada hardware conectado à rede tem um endereço de controle de acesso à mídia (MAC). Você pode filtrar esses endereços MAC para restringir o acesso à sua rede. Consulte sua documentação de usuário para ver informações específicas sobre como habilitar esses recursos. Você também pode utilizar a conta de "convidado", que é um recurso amplamente utilizado em muitos roteadores sem fio. Esse recurso permite que você dê acesso à rede sem fio para visitantes em um canal sem fio separado, com uma senha separada, o que mantém a privacidade das suas credenciais primárias.

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.