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

CIBERSEGURANÇA DURANTE VIAGENS

Nesse mundo em que estamos constantemente conectados, a cibersegurança não pode se limitar à casa ou ao escritório. Quando você viaja, seja uma viagem doméstica ou internacional, é sempre importante praticar um comportamento on-line seguro e tomar medidas proativas para proteger os dispositivos habilitados para internet. Quanto mais viajamos, maior é o nosso risco de ciberataques. Seja ciberesperto (#BeCyberSmart) e use as dicas a seguir para se conectar com confiança quando estiver fora de casa.

DICAS SIMPLES:

ANTES DE IR

- **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 backup das suas informações.** Faça um backup dos seus dados em dispositivos móveis, como contatos, dados financeiros, fotos e vídeos, em outro dispositivo ou em um serviço de nuvem, no caso de o seu dispositivo ser comprometido e você precisar redefini-lo com as configurações de fábrica.
- **Conecte-se apenas com pessoas em quem confie.** Embora algumas redes sociais possam parecer mais seguras devido ao número limitado de informações pessoais compartilhadas nelas, limite suas conexões às pessoas que você conhece e nas quais você confia.
- **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.
- **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.

DURANTE A VIAGEM

- **Pare de se conectar automaticamente.** Alguns dispositivos buscam redes sem fio ou dispositivos Bluetooth disponíveis e se conectam automaticamente a eles. Essa conexão instantânea abre a porta para que os cibercriminosos acessem seus dispositivos remotamente. Desabilite esses recursos para poder escolher ativamente quando se conectar a uma rede segura.

- **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.
- **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. Leia Dicas sobre phishing para obter mais informações.
- **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.
- **Guarde seus dispositivos móveis.** Para evitar roubo e acesso não autorizado ou perda de informações sigilosas, nunca deixe seu equipamento sem supervisão em um local público; isso inclui dispositivos de armazenamento externo ou USB. Mantenha seus dispositivos protegidos em táxis, aeroportos, aviões e no seu quarto de hotel.

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.