A cibersegurança não pode ir de férias

Diário de Notícias · 2024-08-14



---

a descontração não deve significar despreocupação com as sempre imprescindíveis práticas de segurança online.

---

file: 2024-08-14-dn-a-ciberseguranca-nao-pode-ir-de-ferias.md

title: A cibersegurança não pode ir de férias

outlet: Diário de Notícias

date: 2024-08-14

date_display: "14 de agosto de 2024, 21:21 (Europe/Lisbon)"

url: "https://www.dn.pt/opiniao-dn/opiniao/a-ciberseguranca-nao-pode-ir-de-ferias"

author_page: "https://www.dn.pt/author/joao-luis"

byline: João Luís

text_status: full

word_count: 604

section: Opinião

extract: dn

notes: "A página do DN não indica afiliação (Dashlane ou outra). A página de autor https://www.dn.pt/author/joao-luis lista apenas este artigo. O texto é de opinião sobre cibersegurança e recomenda «digital vaults», em linha com os restantes artigos assinados pelo João Luís da Dashlane no mesmo período. Há outra página de autor no DN (`/author/joao-luis-2`) que é de outra pessoa e não foi incluída."

A cibersegurança não pode ir de férias

João Luís

Diário de Notícias, 14 de agosto de 2024, 21:21 (Europe/Lisbon)

https://www.dn.pt/opiniao-dn/opiniao/a-ciberseguranca-nao-pode-ir-de-ferias

As férias são vistas, pela maior parte de nós, como uma altura para desligar do quotidiano e relaxar. Para os cibercriminosos, representam uma oportunidade para explorar vulnerabilidades.

Sendo um período em que, regra geral, as nossas rotinas se alteram e contemplamos algumas viagens no calendário, é também um período em que facilmente baixamos a guarda e nos tornamos mais suscetíveis a ciberataques. O

contacto com ambientes com que não estamos familiarizados, assim como as novas rotinas - que implicam, por exemplo, um elevado número de pagamentos diários -, tornam-nos alvos acessíveis e apetecíveis a ataques como phishing e clonagem de cartões, assim como propiciam roubo (ou perda) de equipamentos e consequente extravio de dados.

Alguns dos riscos mais comuns que podemos enfrentar em férias/em viagem estão relacionados com a utilização de redes Wi-Fi públicas e inseguras (em aeroportos, cafés, etc.), tornando-nos imediatamente suscetíveis a que as nossas comunicações e dados sejam intercetados. Da mesma forma, as estações de carregamento USB disponíveis em locais públicos podem ser utilizadas para roubo de dados por alguém mal intencionado.

Caso suspeitemos de que estamos a ser alvo de um ciberataque e que as nossas informações podem estar comprometidas, para além de reportar o caso às autoridades competentes, devemos desconectar-nos imediatamente de toda e qualquer rede/estação insegura e contactar as linhas de apoio de todos os serviços relevantes, como o nosso banco e serviços de telecomunicações, para solicitar a desativação dos serviços ou a alteração dos dados de acesso (recomendo mesmo ter uma lista, num local seguro, de alguns contactos úteis neste sentido, para este tipo de eventualidades).

Existem algumas recomendações para nos protegermos ao utilizar redes Wi-Fi públicas ou estações de carregamento USB, caso não tenhamos alternativa. Utilizar sempre uma VPN é fundamental, permitindo-nos aceder a qualquer ligação de forma segura, privada e encriptada. Evitar aceder a websites ou aplicações sensíveis (como a nossa conta bancária) a partir de redes públicas é outra das recomendações, assim como desativar a conexão automática dos nossos dispositivos a redes Wi-Fi abertas, prevenindo a exposição inadvertida de todo o nosso tráfego online.

No que diz respeito às estações de carregamento USB, é aconselhável utilizar cabos USB “Power Only” - garantindo que, mesmo ligados a um posto de carregamento público comprometido, não haja a capacidade para transmitir

dados, apenas energia. Preferencialmente, devemos utilizar sempre tomadas elétricas ou um powerbank que levemos connosco para carregar os nossos dispositivos.

As mesmas práticas que devemos ter no dia-a-dia para salvaguardar a segurança dos nossos dispositivos eletrónicos e proteger informações sensíveis também se aplicam quando estamos de férias - com as adaptações necessárias ao contexto em que nos encontramos. Refiro-me, por exemplo, à autenticação de dois fatores, a backups regulares dos nossos dados, à manutenção de todo o software que corre nos nossos dispositivos atualizado, à desativação de todos os serviços de localização para proteção máxima da nossa privacidade e, acima de tudo, à utilização de digital vaults para guardar toda a nossa informação sensível, como passwords e informações bancárias (ao invés de utilizar a memória física dos dispositivos que viajam connosco). Em caso de ciberataque, e admitindo que os danos sejam significativos e haja suspeitas de que o dispositivo tenha sido comprometido, deve ser também considerado um reset de fábrica ao equipamento em questão.

Proteger os nossos dispositivos e, consequentemente, os nossos dados assume-se como de extrema relevância. Particularmente em época de férias, a descontração não deve significar despreocupação com as sempre imprescindíveis práticas de segurança online. Manter a cibersegurança como prioridade é mesmo crucial, para que o descanso e a tranquilidade das férias não se transformem, de um momento para o outro, num grande pesadelo.

Recovery notes

A página do DN não indica afiliação (Dashlane ou outra). A página de autor https://www.dn.pt/author/joao-luis lista apenas este artigo. O texto é de opinião sobre cibersegurança e recomenda «digital vaults», em linha com os restantes artigos assinados pelo João Luís da Dashlane no mesmo período. Há outra página de autor no DN (`/author/joao-luis-2`) que é de outra pessoa e não foi incluída.