

Quando o cibercrime não tira férias: 8 dicas para se manter em (ciber)segurança

dinheirovivo.pt/opiniao/quando-o-cibercrime-nao-tira-ferias-8-dicas-para-se-manter-em-ciberseguranca-16800280.html

3 de agosto de 2023



O arranque oficial das férias começa, para muitos, em agosto. Esta é a época mais aguardada do ano, revelando-se um período naturalmente mais descontraído, já que nos permite sair das nossas rotinas e dar-nos ao prazer de outro tipo de distrações, como seja passar mais tempo com a família e os amigos, visitar locais diferentes e, por regra, estar longe de casa. Em vésperas de entrarmos na famosa e esperada *Silly Season*, nunca será de mais relembrar que é vital não "baixar a guarda" nem tão pouco descuidar os cuidados que habitualmente tentamos colocar em prática na nossa vivência no ciberespaço.

É importante reforçar que o cibercrime não tira férias e espreita sempre ao mínimo deslize. Nesta época, quando a distração individual é mais acentuada, situações como ataques de *phishing*, tentativas de roubo de *passwords* ou informações pessoais sucedem-se com considerável frequência, e, pior, com cada vez maior sucesso e impacto.

Há inúmeros perigos à espreita no mundo digital - por isso, partilho oito dicas úteis e muito práticas que poderão evitar riscos indesejáveis, para que seja possível usufruir ao máximo das suas férias, sem preocupações com o cibercrime.

1. Evite ligar-se a redes Wi-fi públicas

As redes wi-fi públicas, como as dos restaurantes, cafés, hotéis e aeroportos, apresentam níveis de segurança consideravelmente mais baixos do que a sua rede pessoal ou corporativa. Por essa razão, sempre que possível, evite utilizar essas redes, optando, por exemplo, pelo pacote de dados do seu telemóvel. Evite também os acessos remotos aos serviços corporativos da empresa através de equipamentos não confiáveis (ex.: computadores de hotéis, restaurantes, bares, entre outros locais públicos).

2. Evite expor-se nas redes sociais e não partilhe a sua localização geográfica

Uma maior exposição acaba por facilitar a recolha de informação para eventuais ataques personalizados. Neste sentido, evite partilhar fotografias das suas férias ou restrinja essa partilha às pessoas mais próximas, protegendo a sua identidade e outras informações de más intenções. Evite partilhas online que contenham datas e locais específicos de férias.

Subscrever newsletter

Subscreva a nossa newsletter e tenha as notícias no seu e-mail todos os dias

3. Evite abrir mensagens e e-mails de fontes desconhecidas ou suspeitas

Uma das técnicas utilizadas no cibercrime é o envio de mensagens de telefone e e-mails através de remetentes desconhecidos. É possível identificá-los através do recurso à linguagem com erros ortográficos, sentido de urgência (por exemplo, promoções extraordinárias ou que estão quase a terminar, contas que vão expirar se não inserir os seus códigos de acesso, etc.), e ainda com a utilização de links e downloads. Leia com atenção e, na dúvida, não avance e elimine a mensagem ou o e-mail.

4. Evite usar equipamentos tecnológicos em locais públicos

Mantenha os seus equipamentos de trabalho (telefone, computador e tablet) longe dos olhares mais curiosos. Idealmente, opte por utilizar estes equipamentos em ambientes privados e seguros, de forma a evitar a exposição de informação confidencial. A mesma regra aplica-se ainda a ações pessoais como inserção de detalhes bancários ou iniciar sessões nas suas contas. Se tal não for possível, sempre que estiver em lugares públicos bloqueie os seus equipamentos ou utilize a autenticação de dois fatores (2FA).

5. Evite guardar credenciais de contas em locais de férias

Para facilitar o seu manuseamento é possível que tenha a tendência para gravar credenciais dos equipamentos das casas de férias ou hotéis. Não corra esse risco. Contudo, caso isso aconteça, faça a redefinição das suas credenciais (passwords) com a maior brevidade possível.

6. Evite reservar viagens em sites pouco fiáveis

Em caso de viagem ao estrangeiro, marque a estada, viagens e outras atividades lúdicas em sites fidedignos. Antes de avançar com a compra, investigue a empresa responsável por essas reservas. Tenha também em atenção aos modos de pagamento. Idealmente pague via transferência, MBWay ou através de cartões bancários (crédito ou débito) de cariz temporário.

7. Evite utilizar máquinas ATM

A caixa multibanco que escolhe para levantar dinheiro é outro local propício ao cibercrime, em especial nas zonas mais turísticas. Caso necessite de utilizar as máquinas ATM, dê prioridade às que se encontram em espaços seguros, de preferência as do seu banco de confiança.

8. Faça as atualizações dos seus equipamentos

Por último, mantenha as atualizações dos equipamentos de IoT no decorrer do período de férias. Não deixe esta funcionalidade para depois.

A adoção destas boas práticas de cibersegurança poderá ajudar a mitigar o risco de ser alvo de ciberataques que lhe estraguem as tão merecidas férias. Para "desligar" em segurança, previna-se, não facilite e mantenha-se alerta.

Boas Férias e até setembro!

Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise