

"Silly Season" e os perigos que nos esperam Out of Office

dinheirovivo.pt/opiniao/silly-season-e-os-perigos-que-nos-esperam-out-of-office-14964472.html

24 de junho de 2022

Entramos agora na chamada "Silly Season" tão característica destes meses de verão, férias e, por vezes, de desatenção online em que as pessoas se encontram mais suscetíveis a descuidar dos cuidados que habitualmente têm na sua vivência no ciberespaço. Nesta altura, situações como ataques de "phishing", tentativas de roubo de passwords ou informações pessoais, ou ainda, num pior cenário, ataques violentos de "ransomware", sucedem-se com maior frequência.

Um dos casos mais recentes de ataques de "phishing", e que eu já abordei junto de alguns meios de comunicação social recentemente, ocorreu na plataforma de alojamento online - booking.com - através do qual várias reservas falsas foram agendadas através dessa mesma plataforma. Neste caso em específico, o aparente proprietário do alojamento alegava que o cartão utilizado para pagamento se encontrava inválido. Após o novo preenchimento dos dados pelo cliente, num website em tudo semelhante ao booking, o alegado proprietário acaba por ficar permanentemente incontactável, e o cliente vê-se sem a reserva e sem o pagamento de reembolso. Mas este acaba por não ser um caso único. Outros casos semelhantes ocorreram em plataformas como a Delta e a Marriott - plataformas de compra de viagens internacionais - nas quais acabam por ser enviadas várias mensagens de spam ou chamadas falsas aos seus clientes para tentarem ludibriá-los a cometer "erros" que acabam em roubo de credenciais ou dinheiro.

Sendo esta uma altura de pensar e planear as férias, é também o momento de repensar e por vezes, ponderar mudanças na sua vida e carreira profissional. Muitas pessoas utilizam esta época para procurar novas ofertas profissionais, numa perspetiva de mudança de emprego. E até, nesta esfera, as pessoas poderão sofrer o mesmo tipo de ataques.

De acordo com o estudo Brand Phishing Report, o LinkedIn é considerado a marca com o maior número de ataques via "phishing". Em contexto de procura de novo emprego e desafio profissional, estes ataques caracterizam-se pelo roubo de informação confidencial através da partilha dos seus dados pessoais. O mesmo aconteceu com a Indeed, uma plataforma de recrutamento e procura de emprego, através da qual várias mensagens de teor fraudulento foram enviadas através de uma plataforma falsa/paralela muito semelhante à original. Os scammers recorreram à técnica do envio de um email de confirmação do respetivo endereço de email dos utilizadores, sendo posteriormente remetidos para uma página de login falsa - culminando no roubo de dados pessoais dos visados.

Avaliando estes perigos, existem, contudo, várias formas de evitar ser atacado no seu ciberespaço, nomeadamente, através de algumas dicas e conselhos muito simples. Em primeiro lugar, apostar na proteção dos seus equipamentos e aplicações através da correta configuração de software de segurança (ex.: antivírus); em segundo, utilizar o conceito de

múltiplos fatores de autenticação nas várias contas que o utilizador possua, assim como, proteger a sua informação através de cópias de segurança regulares. Ao efetuar uma compra ou uma reserva online, torna-se crucial verificar a segurança/credibilidade do website e/ou o remetente do email; é ainda necessário estar atento aos pormenores do mesmo, em particular, observar os erros gramaticais, caracteres estranhos e sobretudo, a inclusão de links com domínios "suspeitos". É também fundamental não fornecer informações pessoais ou bancárias a websites ou emails pouco fiáveis ou com os quais não sinta total confiança e principalmente, cuja identidade se revele desconhecida ou inexistente, aquando de uma simples pesquisa online.

Em resumo, e em analogia direta com o "mundo real", a minha recomendação passa para que cada um de nós passe a aplicar os mesmos conceitos de "sobrevivência" que aplica no seu dia-a-dia - ex.: não andar em zonas perigosas à noite, não falar com estranhos, desconfiar de comportamentos "estranhos", etc. - ao mundo digital.

Sendo as férias de verão um momento pelo qual todos ansiamos, e apesar de um maior relaxamento, devemos ter atenção redobrada sempre que estejamos online para evitarmos cair nestes esquemas fraudulentos, cada vez mais inteligentes, sofisticados e eficazes, com graves prejuízos para os utilizadores, no fundo, todos nós. Há que reforçar que os perigos iminentes nas redes sociais e em todo o universo online nunca tiram férias.

Bruno Castro, Fundador e CEO da VisionWare - Sistemas de Informação SA.