Kaspersky avisa para comportamentos online que devem ser interrompidos

bit.pt/kaspersky-avisa-comportamentos-online-devem-interrompidos/

Ana Rita Guerra 09/12/2016

Há mais informações pessoais nas redes do que nunca, e por isso a Kaspersky Lab preparou uma lista com 7 comportamentos comuns e perigosos aos quais os utilizadores estão suscetíveis todos os dias. Estas ações, diz a especialista em segurança, devem ser "interrompidas imediatamente."

1. Confiar demasiadamente no Wi-Fi aberto
Redes de Wi-Fi de uma maneira geral representam risco, começando com a confiança depositada na legitimidade dela. Por exemplo, criminosos podem criar um ponto de acesso Wi-Fi e nomeá-lo de maneira plausível como "Wi-Fi aberto McDonalds" ou "Hotel Guest 3".

Caso tenha garantido que uma rede aberta de WiFi é o que parece, não significa que os criminosos não estejam a espiar a rede. Utilize as redes suspeitas da maneira mais segura possível: evite aceder a sites que requeiram inserção de informações de login, assim como não faça qualquer transação financeira. Nada de banco, ou compras. Se possível, use VPN.

2. Escolher senhas simples
Nomes de animais de estimação, aniversários, nomes de familiares, e coisa do género caracterizam as piores senhas possíveis. Em vez disso, tente usar opções difíceis de adivinhar (tanto a Kaspersky Lab como outras empresas têm um password checker para verificar se a senha escolhida é segura).

A boa notícia é que uma senha confiável não precisa de ser algo como ilegível como ML)k[V/u,p%mA+5m – algo completamente aleatório do qual numa se vai lembrar. Experimente técnicas de criação de senhas fortes e fáceis de memorizar.

3. Reutilizar as senhas
Finalmente encontrou uma senha incrível. Forte como um touro. Fácil de lembrar, difícil de descobrir. Adivinhe? Não pare por aí, vai precisar de mais senhas. Porque mesmo que diminua a chance de um hacker adivinhar a sua senha, a chance das suas informações serem comprometidas num hack de base de dados ainda existe, por isso não utilize a mesma senha para todos seus registos.

4. Clicar em links recebidos por e-mail
Quem imaginou que enviar links por e-mails era uma boa ideia? Bem, muita gente – incluindo criminosos. Clicar num link de spam ou phishing pode levá-lo automaticamente para um site que baixará um malware para seu computador ou para um site que pode até parecer familiar, mas que vai roubar a sua senha.

Também não clique em links que servem apenas para atrair likes. Como posts com mensagens como "goste e partilhe para ganhar um smartphone!" No melhor dos casos não ganhará nada, mas é possível que esteja a ajudar criminosos a validarem as suas práticas.

5. Fornecer informações de login a qualquer um
A única forma de ter a certeza de que ninguém mal-intencionado tenha as suas informações é mantê-las para si.

6. Avisar a Internet inteira que vai viajar
"Na praia por duas semanas – inveja?"; "A caminho do México de mañana!"; "Alguém pode cuidar do Rex enquanto fico fora por duas semanas?"; E fotos com geolocalização que mostrem o local onde foram tiradas? Mantenha essa informação apenas para os amigos confiáveis – especialmente, em meios como o Facebook que mostram a sua cidade de residência.

7. Aceitar as configurações de privacidade padrão de redes sociais
Os medias sociais fornecem grande controlo sobre o volume de informações que transmite – para o público e para suas conexões; para terceiros, entre outros. Mas talvez queira investigar melhor e acabe por descobrir que essas configurações podem mudar (como o Facebook) com certa frequência. Antes de registar uma nova conta, tire cinco minutos para ver bem as suas configurações de privacidade. Para contas já existentes, deixe de lado alguns minutos para confirmar se está a partilhar as suas informações apenas com quem quer.

“Então, antes de publicar algo para os seus amigos no Facebook, os seus seguidores no Twitter, as suas conexões no LinkedIn, ou seja, lá para quem mais queira transmitir, pense um pouco só para ter certeza de que não está a enviar a estranhos informações que possam ajudá-los a passarem-se por si ou prejudicá-lo de alguma forma”, dizem os especialistas da Kaspersky.

Na maioria das vezes vale a pena se manter alerta – e desconfiado – com a sua vida virtual, aconselha a empresa. Serviços online de provedores de Wi-Fi até bancos e redes sociais procuram fazer com que o utilizador se sinta confortável, mas para criminosos online, esta inércia é uma oportunidade de fazer dinheiro.