

OUCH!

O boletim mensal de conscientização de segurança para você

Limpeza de primavera

Visão geral

A maioria de nós está ansiosa para a primavera! A paisagem começa a ganhar forma, as flores começam a florescer e, para muitos, há um desejo de se manter limpo. Embora possa ser fácil ver a necessidade de limpar e arrumar, perceber a necessidade de também se organizar digitalmente não é tão claro. Confira algumas dicas rápidas para organizar sua vida digital e estabelecer novos hábitos digitais:



BACKUPS: Listamos essa etapa primeiro pois, em longo prazo, é uma das mais importantes e uma etapa que você quer executar antes de realizar as outras. Não importa o seu nível de segurança, em algum momento, você provavelmente precisará de backups para recuperar suas informações importantes. Os motivos incluem falhas no disco rígido, perda de um dispositivo e infecção por malware como o ransomware. A criação e o agendamento de backups automáticos garantem a recuperação das informações mais importantes.



DELETE: Exclua todos os programas ou aplicativos não utilizados em seus dispositivos móveis e computadores. Alguns aplicativos requerem grandes quantidades de armazenamento, podem causar novas vulnerabilidades e até mesmo deixar tudo lento. Quanto menos aplicativos você tiver, mais seguro serão seu sistema e suas informações. Muitos dispositivos mostram quanto tempo se passou desde que você usou um aplicativo. Se já faz mais de alguns meses, é provável que já não precise do aplicativo!



ATUALIZAR: Atualize todos os dispositivos que você tiver, e ative a atualização automática sempre que possível. Dessa forma, seus dispositivos e aplicativos permanecem atualizados, não só garantindo a execução mais rápida, mas tornando muito mais difícil para alguém invadi-los.



SENHAS: Revise suas senhas. Se estiver usando as mesmas senhas para várias contas, altere-as para que cada conta tenha uma senha exclusiva. Não consegue se lembrar de todas essas senhas únicas? Considere utilizar um gerenciador de senhas. Por último, ative a autenticação de dois fatores(2FA) sempre que possível, especialmente para qualquer email ou conta financeira.



CONTAS FINANCEIRAS: Verifique se suas contas bancárias, contas de cartão de crédito e aposentadoria estão configuradas para alertá-lo sempre que uma transação for feita, especialmente para compras grandes ou transferências de dinheiro. Quanto mais cedo você detectar atividades fraudulentas, mais cedo poderá detê-las. Dependendo do país em que você vive, um congelamento de crédito pode ser uma das maneiras mais eficazes de proteger sua identidade.



NAVEGADOR: Revise todos e quaisquer complementos ou plug-ins instalados no seu navegador. Revise as configurações de permissão; os plug-ins realmente precisam ter acesso à sua localização, senhas ou listas de contatos? Se você não estiver mais usando certos plug-ins ou tiver preocupações com a privacidade, exclua-os.



MÍDIAS SOCIAIS: Verifique sua presença online e assuma o controle. Revise suas configurações de privacidade e exclua todas as fotos e vídeos que não são mais acessados ou necessários. Você também pode procurar por si mesmo em um motor de pesquisa e ver quais informações estão disponíveis sobre você. Lembre-se de que é bom limitar a quantidade de informações que você compartilha e mesmo com quem escolhe compartilhar.



MESA: Limpe a gaveta da sua mesa, limpe todos os discos rígidos e pendrives antigos e talvez até mesmo destrua as notas adesivas com bastante informação. Considere investir em uma trituradora de documentos, se não tiver uma.



E-MAIL: Faça uma limpeza de arquivo de e-mail, exclua o que não precisa e organize o que você faz. Preste atenção especial a quaisquer documentos confidenciais, como aqueles com sua data de nascimento ou número do Previdência Social, e tire-os de sua caixa de entrada!

Embora isso possa parecer uma tarefa assustadora, tenha certeza de que seus dispositivos e informações estarão muito mais protegidos. Se isso parecer muito trabalho, considere escolher só alguns itens ou tente marcar um item por dia ou semana. Cada pequeno passo ajuda a protegê-lo.

Editor convidado

Katie Nickels (@LiketheCoins) é analista principal de inteligência da Red Canary e instrutora do SANS para o FOR578: Cyber Threat Intelligence. Ela trabalha em defesa de rede, resposta a incidentes e inteligência de ameaças cibernéticas há mais de uma década.



Recursos

Tem Backups: <http://www.sans.org/u/ZVr>
Simplificando as senhas: <http://www.sans.org/u/ZVw>
Pesquise a si mesmo online: <http://www.sans.org/u/ZVB>
Descarte de seus dispositivos móveis: <http://www.sans.org/u/ZVG>

OUCH! é publicado pela SANS Security Awareness e é distribuído sob a [licença Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Você é livre para compartilhar ou distribuir este boletim, desde que não o venda ou modifique. Conselho Editorial: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley