PHISHX

Segurança em dispositivos móveis

Atualize frequentemente

O seu celular precisa estar sempre com as versões mais atualizadas do sistema operacional, como o IOS ou o Android, além das atualizações de segurança periódicas que são liberadas pelo fabricante do dispositivo algumas vezes por ano.

Embora seja mais comum os aparelhos antigos da Apple permitirem atualizações recentes, iniciativas de fabricantes em modelos mais novos ou programas como o Android One, que garantem atualizações por pelo menos 2 a 3 anos, devem ser priorizados.

Aplicativo bom é original

Os aplicativos também trazem atualizações e melhorias, como novos filtros de fotos ou funcionalidades, e podem ser atualizados automaticamente ou entrando na loja oficial da Apple App Store ou Google Play. Que tal fazer algumas vezes por mês?

Aplicativos sem custo inicial geralmente são bancados com anúncios e ou venda de informações pessoais para terceiros, como CPF e perfis de consumo e busca.

Cópias, muitas cópias

Uma das recomendações mais fáceis é manter cópias de segurança (backup) de seus dados do celular, como contatos, conversas, fotos e aplicativos. Para isso você geralmente vai ter 3 cópias: no próprio aparelho, no seu computador e em algum outro lugar, como a nuvem.

Existem diversos serviços da própria Apple (iCloud), da Google (Drive) e de terceiros que permitem manter todo o histórico das fotos das últimas viagens e da família toda.

Senhas, muitas senhas

Sim, podemos acessar de forma fácil com a biometria, mas ainda vamos precisar de muitas senhas. Na verdade, o recomendado é ter pelo menos uma senha diferente para cada acesso a aplicativos e sistemas.

Para gerenciar essas senhas e lugares diferentes, existem aplicativos no celular ou computador que armazenam e preenchem as mesmas de forma segura. Vale muito a pena, pelo menos lembre-se disso. Procure indicação de um Gerenciador de Senhas para o seu dispositivo agora mesmo.

2 é ainda mais seguro

Que tal reduzir o risco de incidentes, perda de dinheiros e manter a sua privacidade online? Tudo fica mais fácil quando você habilita em todos os aplicativos, incluindo os financeiros, redes sociais e jogos duas funções essenciais: Verificação em Duas Etapas e Autenticação em Múltiplos Fatores.

A Verificação em Duas Etapas garante que o cadastro de um novo aplicativo vai confirmar que a pessoa tem posse física do aparelho, como a configuração inicial do Telegram.

A Autenticação em Múltiplos Fatores garante que apenas você vai acessar o aplicativo através de biometria, fornecendo sua digital ou rosto em aparelhos que permitem essa funcionalidade. Até o WhatsApp já permite isso. Tá esperando o que?

Sua internet te protege

Eu sei que ajuda usar aquele Wi-Fi da cafeteria, afinal é de graça e as vezes só preciso informar meus dados. Além de podermos conversar depois novamente sobre a sua privacidade, os seus dados, mesmo que um simples check-in valem dinheiro.

O recomendado é sempre optar por usar a Internet do seu aparelho, via rede celular, quando for fazer algo importante, como acessar o seu banco, compras ou o email da empresa.

Além disso, você pode também usar uma camada extra de proteção através de VPN (rede privada) da sua empresa ou particular.