Veja 3 dicas para manter suas fotos seguras na nuvem

Descubra se você está salvando fotos automaticamente na nuvem

Todos os sistemas (iOS, Android e Windows Phone) têm esta opção nativa, mas muitos estão com ela ativada e nem sabem. Usuários do iOS devem acessar a opção de iCloud na área de Ajustes do dispositivo. Lá, entre em Fotos e ajuste a configuração de backup automático, desligando-a se assim for do seu interesse.

Usuários do Android tem a opção de auto-backup pelo Google+. Para ativar ou desativá-la, basta entrar no aplicativo, em Configurações e entrar em Backup automático. Nesta área, você pode selecionar se prefere o recurso ativado ou desativado.

Já no Windows Phone, o backup automático é feito no OneDrive, mas a opção de desligar está dentro da área de Configurações do aplicativo de Fotos.

Para quem usa o aplicativo do Dropbox no celular, independente do sistema, pode entrar na área de Configurações para desativar o recurso.

Autenticação em dois passos

Você deveria ativar isso para qualquer recurso de internet que você puder, pois garante que mesmo que o cibercriminoso tenha sua senha, ele terá que quebrar outra barreira de autenticação quase impenetrável antes de ter acesso aos seus dados. Basta lembrar do token, ou o "chaveiro" que as pessoas costumam receber do banco para acessar sua conta pela internet.

Normalmente o recurso funciona com a geração de um código aleatório enviado para o seu celular, ou então é utilizado um aplicativo como o Google Authenticator, ou o aplicativo do Facebook. Alguns serviços chegam a oferecer um item físico para poder realizar a autenticação mesmo sem um celular.

Não seja enganado

Força bruta e conhecimento técnico são só algumas das possibilidades utilizadas pelo cibercrime. Muitas vezes, a opção mais simples é pedir ao usuário as informações de acesso. Parece fácil fugir do golpe, mas ele normalmente vem mascarado por uma série de truques e as pessoas caem com uma frequência incrível.

Normalmente, o ataque se dá por meio de mensagens enviadas por e-mail, solicitando informações que comprometam a segurança do usuário. Um exemplo simples seria a "Apple" entrando em contato com um usuário por e-mail ameaçando cancelamento da conta caso as informações de cadastro não sejam atualizadas. A mensagem vem com um link para um site que se passa pelo da Apple, onde o usuário deve fazer um "login", que não fará nada além de enviar de seus dados para o cibercriminoso.

Não aceite solicitações de "reset" de senha se você não solicitou nenhuma e não envie seus dados de acesso por e-mail para ninguém. Se você suspeitar de algo estranho acontecendo em sua conta, acesse o site do serviço e entre em "Esqueceu sua senha?" e inicie o processo para mudá-la o mais rápido possível.

Fonte: <http://olhardigital.uol.com.br/noticia/43885/43885> Acessado em: 23 de Setembro de 2014