DINO - Divulgador de Notícias

Autenticação em dois fatores, por que tem se tornado tão necessária para garantir segurança virtual?

Quando se fala de problemas no campo da tecnologia, um dos maiores é sempre a segurança da informação. Por isso, antes mesmo de analisar a questão sobre a perspectiva de futuro é necessário analisar quais as opções atuais que possuímos para uma melhora na segurança virtual.

25/07/2018 13:59:20

Todos os dias, os usuários deixam “rastros” em diversas atividades cotidianas. Quando se dá “likes” ou se compartilha algo em redes sociais, os usuários acabam indicando preferências sobre determinados temas. Ao fazer um cadastro para acessar um site ou serviço na internet, fornecemos identificações importantes, como carteira de motorista e endereço. Ao dar o CPF após uma compra ou para adquirir descontos, fornecemos ao vendedor nossa identificação e informações sobre o que adquirimos e quanto gastamos. Ao usar a digital para entrar em um prédio, deixamos um registro biométrico fundamental sob responsabilidade de empresas e órgãos que, muitas vezes, são desconhecidos.

Os dados são a base de processos da “indústria 4.0” ou “transformação digital”. Segundo o Fórum Econômico Mundial, a transformação digital pode gerar até US$ 10 trilhões anuais na próxima década (R$ 35,4 trilhões, ou 5,3 vezes o Produto Interno Bruto brasileiro registrado em 2017). A Europa projeta um crescimento da sua economia de dados de € 285 para € 739 bilhões entre 2015 e 2020. Com isso, a coleta de dados tornou-se um negócio não apenas de empresas de tecnologia da informação, mas de uma gama variada de setores, provocando preocupações quanto a usos indevidos. Em 2011, a Disney foi multada em R$ 10 milhões por coletar e compartilhar informação de crianças, violando a Lei de Proteção Online da Infância dos Estados Unidos.

A falta de segurança na guarda das informações, uma das dimensões da proteção de dados, também ganhou visibilidade. Em 2017, a agência de crédito Equifax teve dados de 143 milhões de clientes vazados. A firma está sendo acionada judicialmente em processo avaliado em US$ 70 bilhões. Em 2016, um vazamento envolveu informações de 57 milhões de usuários da plataforma de mobilidade Uber, sendo 196 mil brasileiros.

A autenticação em dois fatores (ou verificação em duas etapas) adiciona uma camada extra de segurança quando se faz o login em algum serviço online. Além de fornecer usuário e senha para acessar sua conta, é preciso inserir uma nova informação para confirmar que é você, de fato, que está fazendo o login.

Pâmela Ribeiro, Commercial Strategy Manager da empresa Comtele (www.comtele.com.br) aponta que: ”a verificação em duas etapas já é muito usada para as redes sociais, e-mails ou, até, lojas de comércio eletrônico e o motivo é bastante claro, pois torna a vida dos invasores de plantão mais complicada. Isso porque saber a senha da vítima já não é mais o suficiente para acessar contas alheias. Como é necessário ter as duas combinações em mãos para fazer transações na sua conta, é difícil que alguém leve todo o seu dinheiro caso você perca apenas a sua senha ou apenas o seu token. O mesmo vale na internet: se algum serviço sofrer com problemas de segurança e vazar senhas de usuários, o que não é raro, seus dados continuarão protegidos caso você esteja usando autenticação em duas etapas”.

Embora algumas pessoas ainda insistam em se proteger com apenas uma senha – uma senha frágil, ainda por cima –, a verificação em duas etapas não é nenhuma novidade. Aliás, é bem provável que você já faça uso dessa medida no mundo físico. Mais precisamente nos caixas eletrônicos. Boa parte das empresas já oferece autenticação em duas etapas, incluindo Google, Microsoft, Facebook, Dropbox, Evernote, Apple e Twitter. Depois de ativar a proteção adicional, sistema passa a exigir a digitação de um código adicional, normalmente de seis dígitos, após passar pela tela de nome de usuário e senha, sempre que usar um computador desconhecido.

Por isso, mais do que aplicar a autenticação em dois fatores, uma empresa deve tomar outras medidas de segurança, como procurar trocar senhas com frequência – sem nunca as repetir – e usar senhas alfanuméricas.

Independentemente do tamanho de uma empresa, o duplo fator de autenticação é uma camada de segurança que deve ser considerada, afinal, todos estamos sujeitos a ataques virtuais e roubos de informações e, com o aplicativo, é possível se resguardar de mundo cada vez mais conectado.