Segurança em dois passos?

Nada mais é do que o aprimoramento da segurança tradicional, onde além da senha comum, exige-se outro código. Ou seja, uma camada extra de segurança Mesmo com uma senha fraca, tem-se uma camada de proteção adicional contra crackers. É muito comum você digitar uma senha e o sistema lhe enviar um código para algo que você tenha (um de seus dispositivos celulares, por exemplo).

Outra forma "ainda que relativizada" da segurança dois passos reside nos casos em que o usuário tem registrado seu navegador do computador que usa, sendo que qualquer acesso de outro navegador não será permitido ou exigirá a digitação de um código adicional.

O princípio está relacionado a ideia de que sistemas de autenticação funcionam com confirmação não só de algo que você sabe, mas de algo que você tem ou mesmo, algo que você é… Estes são os fatores de autenticação.

Segundo fator, hoje, é checar algo que você tem! Logins comuns checam apenas o que você sabe e muitas pessoas podem saber o que você sabe…

Algumas empresas que já implementaram a segurança em dois passos são:Apple, Google, Twitter (liberado em maio de 2013), Evernote, Microsoft, Dropbox…

É uma ótima solução contra ataques de pishing. E o exemplo clássico vem dos cartões de banco. Não basta a senha para uma transação bancária, é necessário ou usar um PIN, TOKEN, Cartão com letras ou ainda senha de letras previamente cadastrada. Ou seja, se dificultamos a atuação do criminoso bancário, temos hoje possibilidade de dificultar a atuação de crackers que querem violar nossa privacidade.

Lembrando que nos termos da Lei 12.737/2012 a invasão de

dispositivo informático, mediante violação de mecanismo de segurança, pode configurar crime previsto no art. 154-A, com pena que pode chegar até dois anos de reclusão. Quanto mais caracterizarmos a presença de mecanismos em nossos ativos, menos risco corremos de não sermos protegidos pela Legislação.