OUCH! | Agosto de 2013

A Publicação Mensal de Sensibilização de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Verificação em Duas Etapas

Quem é você ?

O processo de provar quem você é (chamado de autenticação) é um passo fundamental para proteger a sua informação online. Você quer ter certeza de que só você tem acesso às suas informações pessoais, então você precisa de um método seguro para provar quem você é, por exemplo, quando verificar e-mail, comprar algo online ou acessar suas contas bancárias. Você pode provar quem você é de três formas diferentes: o que você sabe, como uma senha, o que você tem, como seu passaporte, e quem você é, como a sua impressão digital. Cada um desses métodos tem as suas vantagens e desvantagens. O método de autenticação mais comum é usar o que você sabe: senhas.

Editor Convidado

James Tarala é palestrante, autor e instrutor sênior do Instituto SANS. Ele é consultor principal de Segurança na Enclave Security e colaborador do Critical Security Controls e **AuditScripts.com**. Você pode acompanhar James no Twitter em **@isaudit** ou conhecê-lo pessoalmente em um de seus próximos cursos.

Senhas

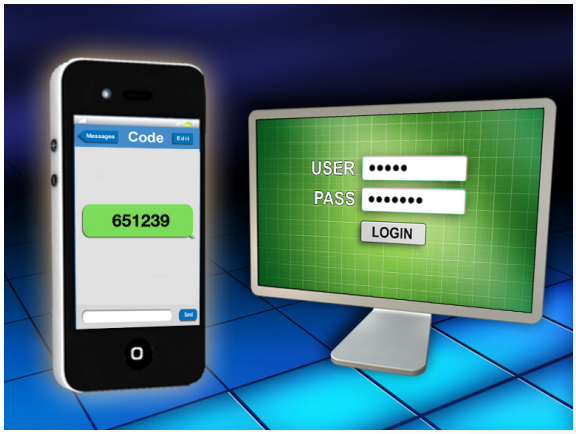
Provavelmente você usa senhas quase todos os dias em sua vida. A finalidade de uma senha é comprovar que você é quem você diz ser. Este seria um exemplo de algo que você sabe. O perigo com senhas é que, se alguém adivinhar ou obtiver acesso à sua senha, esse alguém pode fingir ser você e acessar todas as informações que são protegidas por ela. É por isso que lhe são ensinadas medidas para proteger a sua senha, como o uso de senhas fortes que são difíceis para os atacantes adivinharem. O problema com senhas é que elas estão se tornando ultrapassadas rapidamente. Com novas tecnologias é cada vez mais fácil para os atacantes cibernéticos utilizarem testes de repetição (força bruta) e eventualmente adivinhá-las ou simplesmente colhê-las com tecnologias como grampos de teclado. Uma solução mais simples e ainda mais segura torna-se necessária para autenticação forte. Felizmente, essa opção está se tornando mais comum com uma solução chamada verificação em duas etapas. Para sua proteção, nós recomendamos fortemente que você utilize esta opção, sempre que possível.

Verificação em duas etapas

Verificação em duas etapas (às vezes chamada de autenticação por dois fatores) é uma maneira mais segura para provar a sua identidade. Em vez de exigir apenas um passo para autenticação, tais como senhas (que é algo que você sabe), requer duas etapas. O seu cartão do banco é um exemplo. Quando você retira dinheiro de um caixa eletrônico, na verdade você está usando uma forma de verificação em

Verificação em Duas Etapas

duas etapas. Para provar quem você é ao acessar o seu dinheiro, você precisa de duas coisas: o cartão (algo que você tem) e o número de senha (algo que você sabe). Se você perder o seu cartão do banco seu dinheiro ainda está seguro. Qualquer pessoa que encontre o seu cartão não consegue retirar o seu dinheiro, pois não sabe a sua senha (a menos que você a tenha escrito no seu cartão, o que é uma má idéia). O mesmo é verdade se eles só têm a sua senha e não o cartão. O atacante precisa ter ambos para comprometer sua conta. Isto é o que faz a verificação em duas etapas ser muito mais segura: você tem dois níveis de segurança.



Use a verificação em duas etapas sempre que possível, pois é uma solução muito mais segura do que usar apenas senhas.

Usando Verificação de duas etapas

Um dos líderes na verificação em duas etapas online é o Google. Com uma variedade de serviços online gratuitos, como Gmail, o Google precisou fornecer uma solução de autenticação forte para os seus milhões de usuários. Para isso, o Google lançou a verificação em duas etapas para a maioria de seus serviços online. Não é só o serviço de verificação em duas etapas do Google que pode ser usado gratuitamente. Outros provedores online também estão usando tecnologia similar para seus serviços, como Dropbox, Facebook, LinkedIn e Twitter. Ao compreender como a verificação de duas etapas do Google funciona, você vai entender como muitos outros serviços on-line de verificação de duas etapas funcionam.

Verificação em duas etapas do Google funciona da seguinte maneira. Primeiro, você precisa do seu nome de usuário e senha, exatamente como antes. Esse é o primeiro fator, algo que você sabe. No entanto, o Google requer então um segundo fator, algo que você tem - mais especificamente, o seu smartphone. Há duas maneiras diferentes para usar seu smartphone como parte do processo de autenticação no serviço. A primeira é registrar o seu número de telefone no Google. Quando você tenta se autenticar com seu nome de usuário e senha, o Google envia um SMS com um código novo e exclusivo, para o seu smartphone. Você então tem que inserir esse número ao entrar. A outra opção é instalar o software de autenticação do Google em seu smartphone. O software gera um código único para você. A vantagem deste segundo método é que você não precisa estar conectado a um provedor de serviços, já que o telefone gera um código para você.

A verificação em duas etapas geralmente não é ativada por padrão, você terá que habilitá-la manualmente. Além disso, a maioria dos aplicativos móveis ainda não é compatível com a verificação em duas etapas. Para a maioria dos aplicativos móveis você vai precisar usar senhas específicas do aplicativo, que você

Verificação em Duas Etapas

pode gerar depois de ativar a verificação em duas etapas. Finalmente, você pode ter a opção de criar sua chave de recuperação no caso de você perder o seu smartphone. Recomendamos que você imprima e armazene em um local seguro e trancado.

Recomendamos fortemente que você use a verificação em duas etapas, sempre que possível, especialmente para os serviços essenciais como e-mail ou armazenamento de arquivos. Verificação em duas etapas é muito mais eficiente para proteger suas informações. E os criminosos têm muito mais trabalho para tentar comprometer suas contas.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: **Homero Palheta Michelini**, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

Onde você pode usar a verificação em duas etapas (em Inglês):
http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two+factor-authentication-right-now

Verificação de duas etapas Google:	http://www.google.com/landing/2step/
Glossário de segurança:	http://cartilha.cert.br/glossario/
Termos Comuns de Segurança (em Inglês):	http://www.securingthehuman.org/resources/security-terms
Dica SANS de Segurança do dia (em Inglês):	https://www.sans.org/tip_of_the_day.php

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Katia Lucia da Silva, Rodrigo Gularte, Marta Visser