The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Who Are You
- Passwords
- Two-Step Verification
- Using Two-Step Verification

Two-Step Verification

Who Are You?

The process of proving who you are (called authentication) is a key step to protecting your online information. You want to be sure only you have access to your private information, so you need a secure method to prove who you are, such as when you check email, purchase something online or access your bank accounts. You can prove who you are in three different ways: what you know, such as a password, what you have, such as your passport, and who you are, such as your fingerprint. Each one of these methods has its advantages and disadvantages. The most common authentication method is using what you know: passwords.

Guest Editor

James Tarala is a speaker, author and senior instructor with the SANS Institute. He is a principal consultant at Enclave Security and a contributor to the Critical Security Controls and **AuditScripts.com**. You can follow James on Twitter **@isaudit** or meet him in person at one of his upcoming courses.

Passwords

You most likely use passwords almost every day in your life. The purpose of a password is to prove you are who you say you are. This would be an example of something you know. The danger with passwords is that if someone else can guess or gain access to your password, they can then pretend to be you and access all of the information that is secured by it. This is why you are taught steps to protect your password, such as using strong passwords that are hard for attackers to guess. The problem with passwords is they are quickly becoming dated. With newer technologies it is becoming easier for cyber attackers to forcibly test and eventually guess passwords or harvest them with technologies such as keystroke loggers. A simpler yet more secure solution is needed for strong authentication. Fortunately, such an option is becoming more common -- something called two-step verification. To protect yourself, we highly recommend you use this option whenever possible.

© The SANS Institute 2013

Two-Step Verification

Two-Step Verification

Two-step verification (sometimes called two-factor authentication) is a more secure way to prove your identity. Instead of requiring just one step for authentication, such as passwords (which is something you know), it requires two steps. Your ATM card is an example. When you withdraw money from an ATM machine, you are actually using a form of two-step verification. To prove who you are when accessing your money, you need two things: the ATM card (something you have) and the PIN number (something you know). If you lose your ATM card your money is still safe; anyone who finds your card cannot withdraw your money as they do not know your PIN (unless you wrote your PIN on your card, which is a bad idea). The same is true if they only have your PIN and not the card. An attacker must have both to compromise your ATM account. This is what makes two-step verification so much more secure: you have two layers of security.

Use two-step verification whenever possible, as it is a far more secure solution than just passwords.

Using Two-Step Verification

One of the leaders in online two-step verification is Google. With a variety of free online services such as Gmail, Google needed to provide a stronger authentication solution for its millions of users. As such Google rolled out two-step verification for most of its online services. Not only is Google's two-step verification a free service any Google user can sign-up for, but other online providers are using similar technology for their services, such as Dropbox, Facebook, LinkedIn and Twitter. By understanding how Google's two-step verification works, you will understand how many other online two-step verification services work.

Google's two-step verification works as follows. First, you will need your username and password, just as before. That is the first factor, something you know. However, Google then requires a second factor, something you have -- specifically, your smartphone. There are two different ways you can use your smartphone as part of the log in process. The first is to register your phone number with Google. When you attempt to authenticate with your

© The SANS Institute 2013

Two-Step Verification

username and password, Google will SMS a new, unique code to your smartphone. You then have to enter this number when you log in. The other option is to install Google authentication software on your smartphone. The software then generates a unique code for you. The advantage with this second approach is that you do not need to be connected to a service provider, as your phone generates your code for you.

Two-step verification is usually not enabled by default; it is something you will have to enable yourself. In addition, most mobile apps are not yet compatible with two-step verification. For most mobile apps you will need to use application-specific passwords, which you can generate once you enable two-step verification. Finally, you may have the option of creating recovery keys in case you lose your smartphone. We recommend you print those out and store them in a safe, locked location.

We highly recommend you use two-step verification whenever possible, especially for critical services such as email or file storage. Two-step verification goes much further to protect your information, as criminals have to work much harder to try and compromise your accounts.

SANS Network Security 2013

Join SANS Institute, the world's most trusted source for computer security training, in Las Vegas September 14 - 23 for Network Security 2013! Choose from more than 45 hands-on courses from beginner to advanced levels in IT security, pen testing, forensics, audit, management , and ICS/SCADA. Learn more at http://www.sans.org/info/136317.

Resources

Where you can use two-step verification:	http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two+factor-authentication-right-now
Google Two-Step Verification:	http://www.google.com/landing/2step/
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 3.0 license.
You are free to distribute this newsletter or use it in your awareness program as long as you do not modify the newsletter.
For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis