OUCH! | September 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

Two-Step Verification

Overview

The process of proving who you are (called authentication) is key to protecting your information. Strong authentication attempts to ensure only you can access your information, such as your email, your photos or your bank accounts. There are three different ways to confirm who you are: what you know (such as a password), what you have (such as your driver's license) and what you are (such as your fingerprint). Each one of these methods has advantages and disadvantages. The most common method is passwords, which are something you know. In this newsletter, we are going to teach you how to protect yourself with two-step verification, something far more secure than just passwords and yet very simple to use. To better understand two-step verification, we need to start with passwords first.

Guest Editor

Keith Palmgren has over 30 years of experience in Information Security. He is a SANS Institute Certified Instructor and author of SANS SEC301, a five-day introductory course on information security. When not teaching, Keith focuses on consulting and writing projects. You can follow Keith on Twitter at **@kpalmgren**.

Passwords

Passwords prove who you are based on something you know. The danger with passwords is that they are a single point of failure. If someone can guess or gain access to your password, they can then pretend to be you and access all of your 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 others to guess, using a different password for each account or never sharing your passwords with others. While this advice remains valid, passwords are outliving their usefulness; they are no longer effective in today's modern age. The latest technologies make it far too easy for cyber attackers to compromise passwords. What we need is an easy to use, yet more secure solution for strong authentication. Fortunately, such an option is now commonly available. It's something called two-step verification.

Two-Step Verification

Two-step verification (sometimes called two-factor authentication or 2FA) is a more secure solution than just passwords. It works by requiring two different methods to authenticate yourself. One example is your ATM card. When you withdraw money from an ATM machine, you are actually using a form of two-step verification. You need two things to access your money: your ATM card (something you have) and your PIN number (something you know). If you lose your ATM card, your money is still safe. Anyone who finds your card will not be able to withdraw your money, as they do not know your PIN. (Unless you wrote your PIN on your card, which is a really bad idea.) The same is true if they only have your PIN and do not have 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.

985043
8:27
985043

Use two-step verification whenever possible; it is one of the strongest steps you can take to protect your information.

Using Two-Step Verification

Two-step verification is something you set up individually for each of your accounts. Fortunately, many online services now offer it. One of the leaders in two-step verification is Google. Google accounts are a prime target for cyber attackers, as they offer a variety of free, online services to millions of people around the world. As such, Google needed to provide stronger authentication. It was one of the first organizations to roll out two-step verification for most of its online services. If you understand how Google's two-step verification works, you will understand how two-step verification works for most other sites, such as Twitter, Facebook, Apple, Instagram and many banks.

First, you enable two-step verification on your Google account and register your mobile phone number. Once completed, two-step verification works as follows. You log into your account just as before with your username and password. This is the first of the two factors -- something you know. Google then sends a text message to your mobile phone containing a unique code, specifically, a string of six numbers. Just like your password, you then enter those six numbers on the website. This is the second of the two factors. To successfully log into your account, you have to both know your password and have your mobile phone receive the unique codes. Even if an attacker has your password, they cannot access your Google account unless they also have your phone. To ensure your account is truly secure, Google will send you a new, unique code every time you log in.

There is another option for two-step verification with Google and many other sites. Instead of receiving the unique code via SMS text messaging, you can install an authentication app on your smartphone. The app generates the unique code for you every time you want to log in. The advantage to using a mobile app is that you do not need to be connected to a phone service to receive your unique code; your phone generates it for you. In addition, since the code is generated locally on your phone and not sent to you, it cannot be intercepted.

Remember, two-step verification is not enabled by default; you have to enable it yourself. While two-step verification may seem like more work at first, we highly recommend you use it whenever possible, especially for critical services, such as your email accounts, online banking or storing your files online. Two-step verification goes much further to protect your information than just simple passwords.

Video of the Month

Be sure to check out our free resources, including the blog, webcasts and Video of the Month. This month, we're covering Software Development Life Cycles (DevOps). View the video at http://www.securingthehuman.org/u/2uX.

Resources

Passphrases:	http://www.securingthehuman.org/ouch/2015#april2015
Sites Supporting Two-Step Verification:	https://twofactorauth.org
Stop|Think|Connect:	http://stopthinkconnect.org/2stepsahead
Google Two-Step Verification:	http://www.google.com/landing/2step/
SANS Security Tip of the Day:	http://www.sans.org/tip_of_the_day.php

License

securingthehuman.org/blog   /securethehuman   @securethehuman   securingthehuman.org/gplus