SANS
SECURITY
AWARENESS

OUCH! | December 2017

The Monthly Security Awareness Newsletter for Everyone

OUCH!

## IN THIS ISSUE...

# Lock Down Your Login

## Overview

The process of authentication, or proving who you are, is key to protecting your information, such as your email, social media, or online banking accounts. You may not realize it, but there are three different ways to prove who you are: what you know, such as a password, what you have, such as your driver's license, and some part of you, such as your fingerprint. Each one of these methods has advantages and disadvantages. The most common authentication method is passwords, which are something you know. Unfortunately, using passwords just by themselves is proving to be more and more insecure. In this newsletter, we teach you how to protect yourself and lock down your login with something far better than just passwords. It's called two-factor authentication.

**Guest Editor**

Tiffany Schoenike is the director of campaigns and initiatives at the National Cyber Security Alliance (**@staysafeonline**). In 2016, Ms. Schoenike worked with the White House, government, and industry to develop and launch Lock Down Your Login, a STOP. THINK. CONNECT.™ campaign about two-factor authentication.

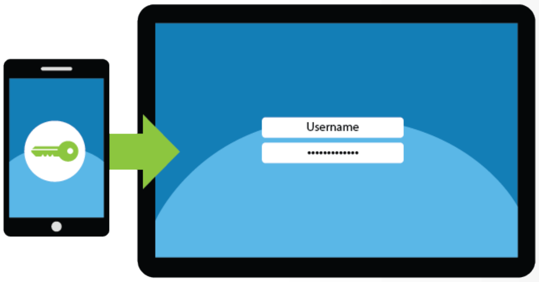
## Passwords Are No Longer Enough

Passwords prove who you are based on something you know. But if someone can guess or gain access to your password, they can then pretend to be you and access all of your information.  Compromised passwords have become one of the leading causes for hacked accounts. This is why you are taught to use passphrases that are hard for others to guess, a different one for every account, and to never share your passwords with others. While this advice remains valid, passwords are no longer as effective. Luckily, there's a simple and quick way to put you in control and keep your personal information safe. It's called two-factor authentication.

# Lock Down Your Login

## What Is Two-Factor Authentication?

Two-factor authentication (also called two-step verification, multi-factor authentication, or 2FA) is far stronger than just using passwords by themselves. It works by requiring not one, but two different methods to prove you are who you say you are. A good example is your ATM card. When you withdraw money from an ATM machine, you are actually using two-factor authentication. To access your cash, you need two things: your ATM card (something you have) and your PIN number (something you know). If your ATM card is lost or stolen, others cannot withdraw your money without also knowing your PIN. A thief must have both your ATM card and pin to make a withdrawal. Two-factor authentication uses the same concept.



*Lock down your login by using two-factor authentication whenever possible. It is one of the strongest steps you can take to protect yourself online.*

## How It Works

Two-factor authentication is widely available on most major banking, email, social networking, and other sites. In addition, most of these sites offer simple step-by-step instructions how to turn on two-factor authentication. (For more information, see the Resources section at the end of this newsletter.) Once you enable two-factor authentication, you can expect it to work like this. First, you log in to your account using your username and password, just as you always have. This is the first of the two factors--something you know. Then you will receive a unique code, often by text to your smartphone. You then enter that code into the login screen. This is the second of the two factors--you must have your phone to receive that code. Now your account is truly locked down. Even if a cybercriminal steals your password, they cannot access your account unless they also have your phone.

Instead of receiving the unique code via text messaging, you can install a special authentication app on your smartphone. This mobile app generates a unique code for you every time you want to log in. The advantage of using a mobile app is it is even more secure, since the code is generated through the app and not sent via text messaging. In addition, it is more convenient, since you do not need to be connected to a phone service to receive your unique code. The app is constantly generating new codes you can use to log in to your account.

While two-factor authentication may seem like more work at first, your personal information will be substantially more secure. Don’t wait until your accounts have been hacked; lock down your login by enabling two-factor authentication on your key accounts, such as email, banking, or social media, and enjoy a greater peace of mind knowing you are far more secure.

## Subscribe to OUCH!

Get the OUCH! security awareness newsletter every month for free, in the language of your choice. Simply subscribe at https://securingthehuman.sans.org/ouch.

## Resources

| | |
|---|---|
| Passphrases: | https://securingthehuman.sans.org/ouch/2017#april2017 |
| Sites Supporting Two-Factor Authentication: | https://twofactorauth.org |
| Stop\|Think\|Connect: | https://www.lockdownyourlogin.org |
| Google Two-Step Verification: | http://www.google.com/landing/2step/ |

## License

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