OUCH! | April, 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Passphrases
- Using Passphrases Securely
- Resources

# Passphrases

## Background

Passwords are something you use almost every day, from accessing your email and banking online to purchasing goods or accessing your smartphone. However, passwords are also one of your weakest points; if someone learns your password, they can steal your identity, transfer your money or access your personal information. Strong passwords are essential to protecting yourself. In this newsletter, you will learn how to create strong passwords that are easy to remember by using a type of password called passphrases.

**Guest Editor**

Guy Bruneau is a senior security consultant with IPSS Inc., a SANS instructor and ISC handler. Guy holds the SANS GSE and completed the SANS Cyber Guardian program. You can follow Guy on Twitter at **@GuyBruneau** and at **handlers.sans.org/gbruneau**.

## Passphrases

The challenge we all face is that cyber attackers have developed sophisticated methods to guess or brute force passwords, and they are constantly getting better at it. This means they can compromise your passwords if they are weak or easy to guess. An important step to protecting yourself is to use strong passwords. The more characters your password has, the stronger it is and the harder it is for an attacker to guess. However, long, complex passwords can be difficult to remember. So instead, we recommend you use passphrases. These are simple phrases or sentences that are easy to remember, but hard to hack. Here is an example:

*Where is king Julian?*

What makes this passphrase so strong is that not only is it 21 characters long, but it also uses capital letters and symbols. (Remember, spaces are nothing more than another symbol.) You can make your passphrase even stronger if you replace letters with numbers or symbols, such as replacing the letter ‘a’ with the ‘@’ symbol or the letter ‘o’ with the number zero. If a website or program limits the number of characters you can use in a password, use the maximum number of characters allowed.

# Passphrases

## Using Passphrases Securely

You must also be careful how you use passphrases. Using a passphrase won't help if bad guys can easily steal or copy it:


*Using passphrases is one of the most effective steps you can take to protect your identity and information.*

1. Be sure to use a different passphrase for every account or device you have. For example, never use the same passphrase for your work or bank account that you use for your personal accounts, such as Facebook, YouTube or Twitter. This way, if one of your accounts is hacked, the other accounts are still safe. If you have too many passphrases to remember (which is very common), consider using a password manager. This is a special program that securely stores all of your passphrases for you. That way, the only passphrases you need to remember are the ones to your computer and the password manager program.

2. Never share a passphrase or your strategy for creating them with anyone else, including coworkers. Remember, a passphrase is a secret. If anyone else knows your passphrase, it is no longer secure. If you accidently share your passphrase with someone else or believe it may have been compromised or stolen, be sure to change it immediately.

3. Just like passwords, avoid easy-to-guess or commonly used passphrases. For example, the phrase, "Four score and seven years ago," is not a good passphrase, since it is so well known.

4. Do not use public computers, such as those at hotels or libraries, to log in to a work or bank account. Since anyone can use these computers, they may be infected with malicious code that captures all of your keystrokes. Only log in to your work or bank accounts on trusted computers or mobile devices.

5. Be careful of websites that require you to answer personal questions. These questions are used if you forget your passphrase and need to reset it. The problem is that the answers to these questions can often be found

## Passphrases

on the Internet, or even on your Facebook page. Make sure that if you answer personal questions, you use only information that is not publicly available or fictitious information you have made up. Password managers can help with this, as many allow you to store this additional information.

6. Many online accounts offer something called two-factor authentication, also known as two-step verification. This is where you need more than just your passphrase to log in, such a passcode sent to your smartphone. This option is much more secure than just a passphrase by itself. Whenever possible, always use these stronger methods of authentication.

7. Mobile devices often require a PIN to protect access to them. Remember, a PIN is nothing more than another password. The longer your PIN is, the more secure it is. Many mobile devices allow you to change your PIN number to an actual passphrase.

8. Finally, if you are no longer using an account, be sure to close, delete or disable it.

## Video of the Month

Be sure to check out our free resources, including our blog and Video of the Month. This month, we're covering Social Engineering from a healthcare perspective. View the video at http://www.securingthehuman.org/u/2uX.

## Resources

| | |
|---|---|
| Two-Step Verification: | http://www.securingthehuman.org/ouch/2013#august2013 |
| Password Managers: | http://www.securingthehuman.org/ouch/2013#october2013 |
| Social Engineering: | http://www.securingthehuman.org/ouch/2014#november2014 |
| Common Security Terms: | http://www.securingthehuman.org/resources/security-terms |

## License