OUCH! | October 2013

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- The Problem
- The Solution
- How Password Managers Work
- Choosing One

Password Managers

The Problem

Often, one of the first things people learn about when protecting their personal identity and information is to use strong passwords. A strong password is one that is not only difficult for cyber criminals to guess, but also resists automated hacking tools. A common rule of thumb is this: the longer and more complex your password is, the stronger and more secure it is. The problem is that strong passwords can be hard to remember. As a result, people often create a single, strong password and use that same password, or slight variations of it, for all of their online accounts, applications and devices. Even more dangerous, many people use the same password for both their personal and work accounts. If you are one of those people reusing your password for multiple accounts, you are at risk. Once a cyber attacker gains access to your password, they can potentially gain access to all of your shared accounts. Ultimately, what you need is a strong and unique password for each of your accounts. That way, if someone gains access to the password for one of your accounts, your other accounts are still secure. Unfortunately, with so many different devices and accounts it has become almost impossible for anyone to remember their growing collection of passwords.

Guest Editor

George Bakos is Technical Director of Intelligence & Response for Northrop Grumman and has been a Certified Instructor with the SANS Institute since 2001. George will be in London this November teaching Security 502, Perimeter Protection in Depth.

The Solution

One solution people often use is to write all their passwords down on a piece of paper, or even worse, write them down and then stick them on their computer monitor. (Ever look in the windows of closed office buildings and seeing monitors plastered with stickies?) This is poor security, as other people can find and read your passwords, especially if you travel and lose them or have them stolen. Instead, what we need is a solution that securely stores all of your passwords in a single location. Even better would be a computer program that simplifies the whole process by automatically retrieving your passwords and logging into websites and applications for you. Better still would be a program that could also generate strong passwords, and perhaps even store other confidential information such as your credit cards. Fortunately, such a solution exists: it is called a password manager (or sometimes a password vault).

Password Managers

How Password Managers Work

A password manager acts like a virtual safe. You first install this virtual safe as a program onto your computer or mobile device. It then takes all of your usernames and passwords and encrypts them in a database, which is then stored on your device or in the cloud. This database is then secured by a special password that you create just for the password manager. This way, you only have to remember one password: the password for your password manager. Anytime you need to retrieve your credentials, such as to log in to your online bank or email accounts, you simply type the password into your password manager. This enables you to have a unique password for every account, even if you have hundreds of accounts, without needing to remember or even see any of them. Since the password manager stores all this sensitive information, you need to be sure that the master password you use is very strong and one that you will not forget.

Password managers are a simple way to securely store all of your different passwords for each of your different accounts.

Many modern password managers can also integrate with your browser. When you visit a website, such as your favorite online store, the password manager will automatically log in for you. If you change your password for that site, the password manager updates the entry for it, as well. Some password managers also work on mobile devices. However, most of these do not work with other mobile apps; they only integrate with your mobile device's browser.

Choosing a Password Manager

There are many free, open source and commercial password managers to choose from. When trying to find the one that's best for you, please keep the following in mind:

- Use only well-known and trusted solutions. Be wary of solutions that have not been around for long or that have little or no community feedback. Cyber criminals can create fake solutions designed to steal your information.
- Make sure whatever solution you choose continues to be actively updated and patched, and be sure you are always using the latest version.

Password Managers

- It should be simple for you to use. If you find the solution too complex to understand, it is easy to make mistakes.
- It should encrypt your passwords using industry standard, strong encryption. Be wary of any solution advertising a proprietary or unknown encryption solution.
- It should run on all the different computers you use. Some more advanced versions also work on mobile devices.
- A helpful feature is if your vault provides a means for synchronizing it across the different devices that you use. If it provides a means for synchronizing, it should encrypt locally before sending to the central system.
- It should provide tools for generating arbitrary passwords and help manage password expiration dates.
- It should help you identify the relative strength of the passwords you've chosen.

Special Webcast - Tuesday, October 29 at 4:00 PM EDT

Join us for a session presented by Alan Paller, SANS Director of Research, where he interviews the Iowa Counties Information Technology Team (ICIT). Hear how they established a unique new model for IT and cyber security cooperation. To date this group of dedicated professionals have completed 11 security projects to assist neighboring counties with limited or no IT resources. The ICIT members have all volunteered their time in helping other counties solve particular cyber security challenges. They have established standardized repeatable measurable processes and would like to share these best practices with other states in an attempt to help county and local government organizations become safer, faster. For more information and to register visit https://www.sans.org/webcasts/iowa-counties--paying-97330.

Resources

Password Manager Review:	http://www.pcmag.com/category2/0,2806,2403435,00.asp
Should I Change My Password?	https://shouldichangemypassword.com/all-sources.php
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

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