The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Strong passwords you can remember
- Never share your passwords
- Using your passwords safely

Protecting Your Passwords

GUEST EDITOR

Eric Cole is the guest editor for the May issue of OUCH! Dr. Cole is the founder of Secure Anchor Consulting, has been the CTO of several large organizations, and is a SANS faculty fellow. He is passionate about helping organizations do the right things to improve their security. You can find out more information at **www.securityhaven.com**.

OVERVIEW

Passwords are the keys to your kingdom. Combined with your username, they are the most common means for proving your identity and logging into your computer and websites or accessing information. Unfortunately, far too often people do little to protect their passwords, using simple combinations such as 123456, password, qwerty, or abc123. In other cases, people simply use their pet's name or their birth date -- information that can be easily found on the Internet, such as on Facebook. With access to your password, an attacker can steal your digital identity, access your bank accounts, or even access your organization's confidential information, causing a tremendous amount of harm. It is also important to remember that if someone steals your password, you could be liable for anything they do! To better protect you, your family, and your organization, let's learn what makes a good password and how to use it safely.

STRONG PASSWORDS

Cyber criminals have developed programs that automate the ability to guess, or brute force, your passwords. To protect yourself, your passwords must be difficult for others to guess but at the same time easy for you to remember. Here is some guidance we recommend.

- You must have at least one number in your password.
- You must have at least one CAPITAL letter in your password.
- You must have at least one symbol in your password.
- We recommend your passwords be a minimum of 12 characters in length. For highly confidential sites or information, we recommend 15 characters. Check with

Protecting Your Passwords

your supervisor for specific policies your organization may have about passwords.

At first glance this approach looks very difficult. However, by using the first letter of each word in a sentence, it becomes much easier to remember: For example, the sentence below may be very simple for you to remember:

My 2nd son was born at Boston Hospital at 6:30pm

However, we can use that sentence to create the password you see here.

M2swb@BH@6:30pm

What we did was simply use the first letter from each word. We capitalized some of these letters. In addition, we replaced the word "at" with the symbol "@." Finally, we included the time at the end. This is a long, complex password that will be very difficult to guess but simple to remember.

PROTECTING YOUR PASSWORDS

Keep in mind that just having strong passwords is not enough. It does not matter if you have the most complex passwords in the world; failing to take the following steps can result in your passwords being compromised:

The key to protecting your passwords is to use strong passwords that are hard to guess, never share them with anyone, and be careful how you use them.

1. Do not get hacked! One of the most common ways for cyber criminals to steal your password is to infect your computer. Once your machine is compromised, bad guys will install specialized malware on it that captures all of your keystrokes, including any usernames and passwords to online banks. When you log in to your bank, your information is automatically stolen and forwarded to the cyber criminals. These individuals can then access your bank account pretending to be you and literally steal all of your money. To protect yourself, make sure your computer is actively protected. This means making sure automatic updating is enabled and you have the latest anti-virus.

Protecting Your Passwords

2. Be sure to use different passwords for different accounts. For example, never use the same passwords for your work or bank accounts as your personal accounts, such as Facebook, YouTube, or Twitter. This way if one of your passwords is hacked, the other accounts are still safe.

3. Never share your password with anyone else, including a supervisor or an IT support professional. Remember, your password is a secret. If anyone else knows your password, it is no longer secure.

4. Never use a public computer, such as at hotels or libraries, to log into an account. Since anyone can use these computers, they may be infected with a malicious code that is capturing all your keystrokes. Only log into your work or personal accounts on trusted computers you control.

5. At times you may have so many passwords that you cannot remember them all, and storing them may be your only option. If you write them down, be sure to store them in locked location that only you have access to; never store them in public view. Another option is to store them in encrypted applications designed to store passwords on your computer or smartphone. Examples of such tools can be found at http://preview.tinyurl.com/622v9m2 and http://preview.tinyurl.com/2p385o.

6. Exercise caution when websites require you to answer personal questions. These questions are often used if you forget your account password and need to reset it. The problem is the answers to these questions can often be found on the Internet, such as your personal Facebook page. So make sure that if you answer personal questions, you use only information that is not publicly known. If the website provides other password reset options, such as SMS messages to your smartphone, you may want to consider these alternatives.

7. If you believe your password has been compromised or have reason to believe it is no longer a secret, contact your help desk and change your passwords immediately from a computer you control and trust.

LEARN MORE

Subscribe to the monthly OUCH! security awareness newsletter, access the OUCH! archives, and learn more about SANS security awareness solutions by visiting us at http://www.securingthehuman.org.