CYBER SECURITY

newsletter

EIGHT STEPS TO PROTECTING YOUR PASSWORDS

Problem

Passwords have become a critical part of our daily lives. You use passwords to logon to your computer, read your email, update your finances, shop online, and even watch movies. It seems that to do almost anything on the Internet today requires some type of password. As a result, your passwords represent the key to your information.

Cyber criminals know this. If they can get your password, they can have access to your bank accounts, read your email, steal your money, sell your information, or even steal your identify. To help you protect yourself, we cover eight simple steps to protecting your passwords.

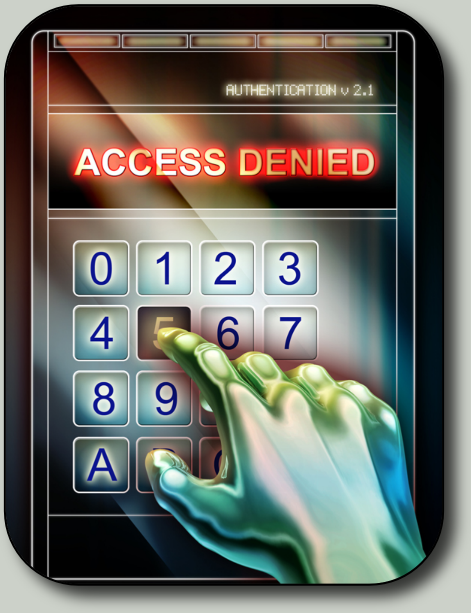
Solution

1. Strong Passwords: Use passwords that are hard to guess. A common way criminals break into accounts is by simply guessing your passwords. On page two, we explain how to create strong passwords that are easy for you to remember but hard for cyber criminals to guess.

2. Use Different Passwords: Use different passwords for different accounts. For example, never use the same password that you use for social networking sites that you use for your online banking or work. This ensures that if one of your passwords is lost or stolen, the rest of your accounts will remain safe.

3. Do Not Share: Never share your password with anyone else; no person or organization (including your bank or your supervisor) needs to know your password. If you do accidently share your password with someone, be sure to change it right away.

4. Untrusted Computer: Never use your passwords on an untrusted computer. An untrusted computer is a public computer that anyone can use. These include computers located in libraries, airports, cyber cafés, hotel lobbies and kiosks. Public computers can easily be infected by cyber criminals who want to steal your passwords. If you accidently use your passwords on a public computer, be sure to change these passwords as soon as possible from your personal computer.



Protecting Your Passwords

Your passwords are the keys to your kingdom, so protect them wisely. Follow these eight steps in order to protect your passwords.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

© The SANS Institute 2011

Strong Passwords

The first step to protecting your passwords is to create passwords that are hard to guess. Criminals will often try to guess your passwords or use automated programs to crack your passwords. Some key points to creating strong passwords are as follows:

- *Do not use simple words that can be found in a dictionary.*
- *Do not use known information about you, such as your name or birthday.*
- *Do make sure to make at least one character a capital letter, one character a number, and one character a symbol.*

All this may seem hard to remember, but there is a trick. Create sentences that are simple to remember, but substitute numbers and symbols for letters. For example, if you can easily remember the saying My 1st son was born at Fairfax Hospital at 11:25, here is an easy way to use it as a strong password.

M1swb@FH@11:25

Here we spelled our sentence but used the first letter of every word. In addition, we made the first letter capital, we replaced the word 'at' with the symbol '@', and then included the time. As a result, this password is very easy to remember, but very difficult to guess.

5. Your Computer: One of the most common ways criminals gain access to your password is by hacking your computer. Once your system is infected they install malware that captures all of your online activity, including your keystrokes. These programs watch whenever you log into a bank or financial site, they then capture all your password credentials. Criminals then use that information to login themselves and steal your money or identity. Often one of the most effective ways to protect your passwords is protect your computer, including make sure it is always updated, has current anti-virus and your firewall is enabled.

6. Phishing Attacks: A phishing attack is when criminals send you bogus messages asking you for your password. These are usually emails that pretend to come from an entity you trust, such as your bank or your favorite online store. The email often says that for security reasons, the business needs you to change your password and ask you to log on to a website. These websites are actually created by the criminals. These websites appear to be legitimate, but they are actually fake, designed only to capture and steal your passwords. Criminals can also use other technologies, such as voice messages, SMS , Facebook, or instant messaging to ask you for your passwords. No legitimate organization needs to know your passwords, so you should never give them away.

7. Password Questions: When you create a new account at websites, one of the things they ask you during the account creation process is to answer some simple questions. The purpose is if you forget your password you can automatically reset your account by answering the personal questions. The danger is, these questions are really nothing more then another type of password. If you answer questions about yourself with information that people can learn about you online (such as Facebook), then they can hack your account. Only answer such questions with information that is not publicly available.

8. Storing Passwords: One of the greatest challenges with passwords can be trying to memorize them all. Often people have too many accounts and passwords to remember. If you need to store your passwords, be sure you do it safely.

If you need to store your passwords there are special security programs designed just for this. They store all your passwords in an encrypted program. You only need to remember one password to open and close the program. Such programs exist for both your computer and mobile devices. To learn more about password storing options, please check with your IT help desk or information security team.

© The SANS Institute 2011