CYBER SECURITY Newsletter

PROTECTING YOUR PASSWORDS

Problem

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

Cyber criminals know this. If they can obtain your passwords, they can have access to your bank accounts, read your email, steal your money, sell your information, or even steal your identify. To help protect yourself, we cover key steps to protecting your passwords in this newsletter.

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 you use for social networking sites as you use for your online banking or work. This ensures if one password 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 be easily 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 steps to protect your passwords.

Idaho State University

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

© The SANS Institute 2012

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 public information about you, such as your pet's name or birthday.*
- *Do make sure to include in your password at least one capital letter, one number, and one symbol.*

All this may seem hard to remember, but there is a trick. Create simple sentences that are easy to remember but substitute numbers and symbols for letters. For example, if you can easily remember the saying, "My favorite food is chocolate," here is an easy way to use it as a strong password.

MyF@v0rit3FoodIsCh0c0l@t3

Here we spelled our sentence, but capitalized the first letter of every word. In addition, we replaced 'a' with '@', 'e' with '3' and 'o' with '0'. 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, capturing all of your online activity, including your keystrokes. These programs watch whenever you log into a bank or financial site and then they capture all your password credentials. Criminals then use that information to log in themselves and steal your money or identity. Often, one of the most effective ways to protect your passwords is to protect your computer by ensuring it is always updated, has current anti-virus, and your firewall is enabled.

6. Password Questions

When you create a new account via a website, they may ask you to answer some simple questions during the set-up process. The purposes of these questions are to help you automatically reset your account if you've forgotten your password. The danger with these questions is that they are really nothing more than another type of password. If you answer questions about yourself with information people can learn about you online (such as Facebook), they can hack your account. Only answer questions with information that is not publicly available.

7. Two-Factor Authentication

Some websites, such as gmail.com, support something called two-factor authentication. This is when you not only need a password to log in, but you need a code. This one-time code is often sent to you via an SMS text message, or perhaps you even installed a special app on your mobile device. You must have both your password and the one-time code to log in. This is a far more secure way to log in to a website. If your password is stolen or compromised, attackers still cannot log in, as they do not have the codes. If a website offers two-factor authentication, we highly recommend you always use it

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.

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 2012