Choosing and Protecting Passwords

Why do you need a password? Think about the number of PIN numbers, passwords, or passphrases you use every day: getting money from the ATM or using your debit card in a store, logging on to your computer or email, signing in to an online bank account or shopping cart...the list seems to just keep getting longer. Keeping track of all of the number, letter, and word combinations may be frustrating at times, and maybe you've wondered if all of the fuss is worth it. After all, what attacker cares about your personal email account, right? Or why would someone bother with your practically empty bank account when there are others with much more money? Often, an attack is not specifically about your account but about using the access to your information to launch a larger attack. And while having someone gain access to your personal email might not seem like much more than an inconvenience and threat to your privacy, think of the implications of an attacker gaining access to your social security number or your medical records.

One of the best ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that someone is the person they claim to be is the next step, and this authentication process is even more important, and more difficult, in the cyber world. Passwords are the most common means of authentication, but if you don't choose good passwords or keep them confidential, they're almost as ineffective as not having any password at all. Many systems and services have been successfully broken into due to the use of insecure and inadequate passwords, and some viruses and worms have exploited systems by guessing weak passwords.

How do you choose a good password? Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to guess or "crack" them. Consider a four-digit PIN number. Is yours a combination of the month, day, or year of your birthday? Or the last four digits of your social security number? Or your address or phone number? Think about how easily it is to find this information out about somebody. What about your email password—is it a word that can be found in the dictionary? If so, it may be susceptible to "dictionary" attacks, which attempt to guess passwords based on words in the dictionary.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "IlTpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Change the same example we used above to "Il!2pBb." and see how much more complicated it has become just by adding numbers and special characters. Don't assume that now that you've developed a strong password you should use it for every system or program you log into. If an attacker does guess it, he would have access to all of your accounts. You should use these techniques to develop unique passwords for each of your accounts. Here is a review of tactics to use when choosing a password:

- Don't use passwords that are based on personal information that can be easily accessed or guessed
- Don't use words that can be found in any dictionary of any language
- Develop a mnemonic for remembering complex passwords
- Use both lowercase and capital letters
- Use a combination of letters, numbers, and special characters
- Use different passwords on different systems

How can you protect your password? Now that you've chosen a password that's difficult to guess, you have to make sure not to leave it someplace for people to find. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, is just making it easy for someone who has physical access to your office. Don't tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords.

If your Internet service provider (ISP) offers choices of authentication systems, look for ones that use Kerberos, challenge/response, or public key encryption rather than simple passwords. Consider challenging service providers who only use passwords to adopt more secure methods.

Also, many programs offer the option of "remembering" your password, but these programs have varying degrees of security protecting that information. Some programs, such as email clients, store the information in clear text in a file on your computer. This means that anyone with access to your computer can discover all of your passwords and can gain access to your information. For this reason, always remember to log out when you are using a public computer (at the library, an Internet cafe, or even a shared computer at your office). Other programs, such as Apple's Keychain and Palm's Secure Desktop, use strong encryption to protect the information. These types of programs may be viable options for managing your passwords if you find you have too many to remember.

There's no guarantee that these techniques will prevent an attacker from learning your password, but they will make it more difficult.