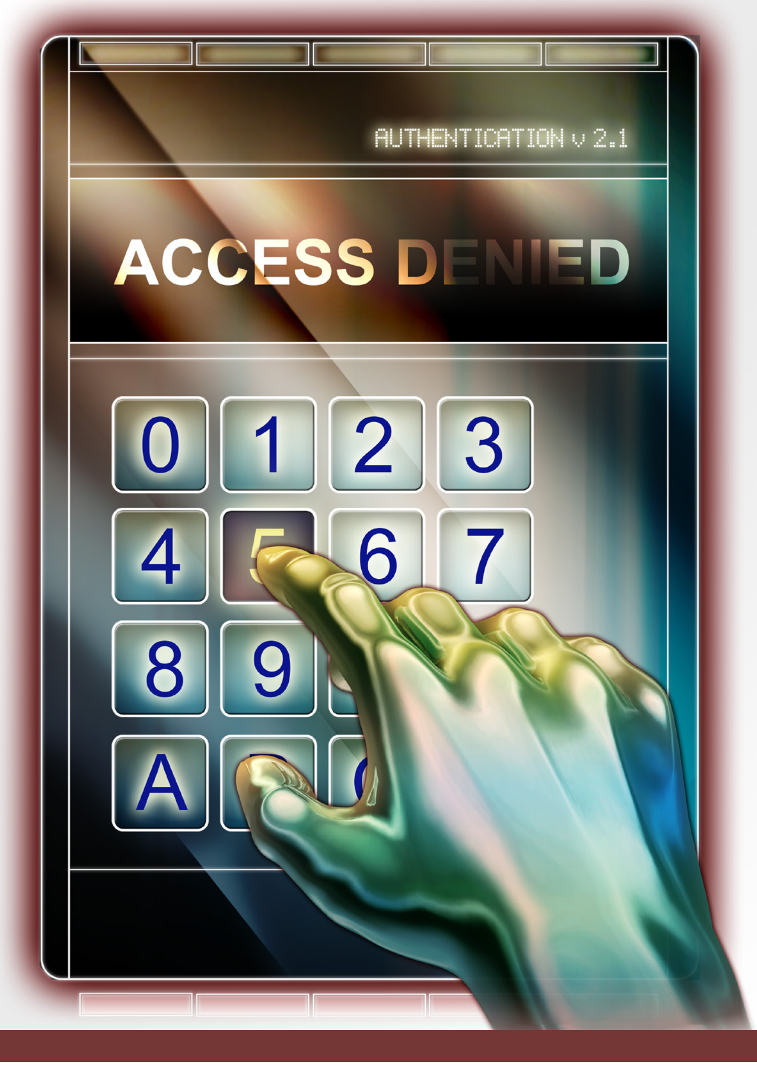
Passwords

Passwords are the keys to your kingdom. You must use them wisely. In this newsletter, we discuss how to create strong passwords that cyber attackers cannot easily guess and cover how to use them securely.



This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu

UNIT INNOVATIVE TECHNOLOGY SOLUTIONS & SERVICES

Passwords

Once someone knows your password, they can steal your identity or access all of your personal information. Let's learn what makes a good password and how to use them securely. There are two key points to good passwords:

- First, you want passwords that are hard to guess. This means do not use simple passwords such as 123456, your pet's name or your birth date.
- Second, use passwords that are easy to remember. If you keep forgetting your passwords, they are not very helpful.

The problem is cyber attackers have developed sophisticated programs that can guess, or brute force, your passwords, and they are constantly getting better at it. This means they can break into your accounts if your passwords are weak. To protect yourself, you want your password to be as long as possible. The longer your password is, the stronger it is. In fact, instead of using just a single word as your password, use multiple words. This is called a passphrase. For example, your passphrase could be something simple like:

Where Is My Coffee?

To make your passphrase even more secure, consider doing the following:

- Use a number in your passphrase.
- Have at least one lowercase and one uppercase letter in your passphrase.
- Use a symbol in your passphrase.

For example, you can replace the letter 'o' with the number zero or the letter 'e' with the number three. In addition, you are using symbols when you use common punctuation such as spaces, a question mark or an exclamation point. As a result, you can have a strong password that is very difficult for cyber criminals to compromise, yet is simple to remember and easy to type. In addition to strong passwords, you must protect how you use them:

- Be sure to use different passwords for different accounts. For example, never use the passwords for your work or bank accounts for your personal accounts, such as Facebook, YouTube or Twitter. This way, if one of your passwords is hacked, the other accounts are still safe. Never share your password with anyone else, including fellow coworkers. Remember, your password is a secret; it is no longer secure if anyone else knows it.

- Do not use public computers, such as those at hotels or libraries, to log into a work or bank account. Since anyone can use these computers, they may be infected with malicious code that captures all of your keystrokes. Only log into your work or bank accounts on trusted computers or mobile devices you control.

- If you accidently share your password with someone else, or believe your password may have been compromised or stolen, be sure to change it immediately.
- Be careful of websites that require you to answer personal questions. These questions are used if you forget your password and need to reset it. The problem is the answers to these questions can often be found on the Internet or your Facebook page. Make sure that you use only information that is not publicly known if you answer personal questions.
- Many online accounts offer something called two-factor authentication, or two-step verification. This is where you need more than just your password to log in, such as codes sent to your smartphone. When possible, always use these stronger methods for authentication.
- Finally, if you are no longer using an account, be sure to disable or delete it.

Password Managers

One of the key points we covered in this newsletter was using a different, unique password for each of your accounts. This way, if one account is compromised, your other accounts are still secure. However, you may have so many accounts you cannot remember all their passwords. If that is the case, consider using a password manager. This is a special program you run on your computer that securely stores all of your passwords for you. The only passwords you need to remember are the ones to your computer and your password manager program. Some password managers even integrate with your browser, logging into websites for you. Check with your supervisor, the help desk or the information security team to see if a password manager is an option you can use.

This newsletter is published by Villanova University's security team.
For more information, please contact us at:

support@villanova.edu