Information Technology Services

Information Security Awareness Program

This document is part of a collection of documents that make up the Information Security Awareness Program. The following is a link to the main Information Security Awareness Program document.

Username & Password Security

A username uniquely identifies you in a system. When that username is combined with a password, it gives you access to systems and data. Often, the data in these systems range from public/non-securable to sensitive/highly-securable. See the Information Security Awareness document Sensitive Data.

Credentials

Together, your username and make up your network or system credentials. It is critically important to take necessary steps to secure your system credentials.

Username security is often overlooked when thinking about security while online, with more emphasis given to passwords. An easy step to take to keep your username secure is to not let your computer automatically remember your username. If someone gains access to this, they have one of two pieces of data they need to impersonate you.

Usernames aren't typically highly securable pieces of data. An example of this is usernames here at Cincinnati State. *John Doe* could have a username of *john.doe*. In this example, if you know John's name, you can easily determine his username, resulting in a very low securable piece of information. A password must be combined with a username to gain access to system or data. This makes your password a highly-securable piece of information and should be protected.

Strong Passwords

Strong passwords are very important in keeping your system credentials safe. Below are a few suggestions that can help you create strong passwords.

- **Length:** Make sure the length of your passwords are eight or more characters
- **Complexity:** Include special characters such as punctuation, symbols, and numbers. Use the entire keyboard, not just the letters and characters you use or see most often. The greater the variety of characters in your password, the better. Example: **Fw8!vZ#pP4***
- **Variation:** To keep strong passwords effective, change them often. Set an automatic reminder for yourself to change your passwords every three months.
- **Variety:** Don't use the same password for everything. Cybercriminals steal passwords on websites that have very little security, and use that same password in more secure environments, such as banking websites.

Never write down your password and store it in a non-secure location. Have you ever wondered how strong your password is? Test the strength of your password on Microsoft's Safety & Security Center.

Secret Questions

Websites often ask you to provide an answer to one or more secret question(s). It is important to use information that isn't readily available from your Facebook, Twitter, or LinkedIn accounts. If you use readily available secret questions, your credentials could easily be compromised.

Never use "Save my password"!

Many websites have the feature to automatically save your username and password. Although this is convenient, it is extremely insecure! It is very easy for someone to sit at our computer and access your systems. You should never have websites or systems remember your passwords automatically.