Password Safety

In today’s online world, strong passwords are essential. Most workplaces and organizations store sensitive information and require usernames and passwords to keep that information safe. Follow these password safety tips and guidelines:

**Create complex passwords**

Strong passwords are 8-16 characters long and use combinations of uppercase and lowercase letters, numbers and punctuation. Spread special characters throughout the password to ensure maximum security. Add emoticons if possible. They can make a password more memorable and boost its strength.

- Avoid:
  - Common or dictionary words (regardless of language) and misspellings
  - Phrases
  - Personal information, such as addresses, birthdays, phone numbers and favorite sports
  - Capitalizing the first letter of the password and putting the special characters on the end
  - Quotes
  - Lyrics

**Use a different username and password for each account**

When hackers compromise one site, they are often able to access many accounts. Using different usernames and passwords can keep other accounts secure, even if one is compromised.

**Keep passwords secure**

Consider using a password manager. Password managers encrypt all of the passwords in the account and can generate complex passwords. Some web browsers offer the option to add these as an extension. Before using a password manager, research it to ensure it practices good encryption and safety policies. Another option is to write passwords down and place them in a secure spot away from the computer. When writing passwords down, do not write the exact username for the account. Instead, write helpful reminders, tips and nicknames that are personal.

**Use a two-factor authentication system**

A two-factor authentication system gives users the ability to receive an email, text or phone call with a verification code after the initial password is entered. Search the network’s help page or contact the system administrator for more details.

**Create unique security questions and answers**

Many applications and services offer the opportunity to create or answer security questions. This method helps recover passwords or acts as a secondary means of logging in. A typical question could be, “What street was your childhood home on?” It is important to add personal, memorable and creative answers and questions.

**Always log out**

Public computers, public Wi-Fi and shared computers are susceptible to privacy attacks. Staying logged in means anyone can see sensitive data and have access to it. Avoid accessing sensitive information when using public services, and always log out when finished on a site.