CGNET
www.cgnet.com

# Top Tips for Cyber Safety

## NEVER:

**Share your password.** With anyone!

**Give remote control** of your computer to someone you don't know.

**Send confidential information via email** (if you must, consider an encryption service such as Privnote or SafeNote).

**Immediately hit "Reply" to an email requesting payment** (gift card purchase; wire transfer) . Contact the supposed sender by another means and verify!

**End a sensitive server session** (such as a bank account) without first signing out or exiting the browser.

**Click a link in an email** unless you are 100% certain you know the sender and/or were expecting a link to be sent.

## ALWAYS:

**Use a strong, complex password**: a combination of upper and lower case letters, numbers, and symbols.

**Protect your home Wi-Fi network** with a strong password and WPA2 encryption.

**Set up two-factor authentication** for your personal accounts such as credit card and bank accounts.

**Confirm that the email address (@domain.org) matches the name of the organization sending you the message**, especially if the message asks you to click on a link.

**Let IT know if you think you received a suspicious message.** Definitely let IT know if you *clicked on a link* in a suspicious message!

## CONSIDER:

Whether an email is trying to **appeal to your emotions** (guilt, urgency) to get you to reply. These are signs of phishing!

Using **a password manager service** to generate and safely store complex passwords for you.

Using **a long passphrase** if you are relying on memory. For example, a quote from a favorite book or film.

Whether **personal information you share on social media** (pet name, favorite band) could be used to personalize a phishing attempt against you.

Using **a VPN service** in a public setting (airport, hotel) if you need to transmit sensitive data safely.

***Remember: YOU are the front line for information security!***