# Cyber Security

By Jarred Demoret

Communication via the internet has become overwhelmingly dominate in our society. Whether you are using Facebook, Twitter, Facetime, or E-mail, odds are it has become a staple in your life. As we go about our daily digital routine, how much thought do you give your personal security? Sure, we don't provide people with passwords to our accounts, however, with very little effort this information can be obtained. Let's look into how to avoid this scenario as well as other preventative measures we can take to stay on-top of our cyber security game.

- Passwords
  - Passwords are generally our first line of defense against cyber criminals. Here are some things to think about when creating or updating passwords that protect our personal accounts:
    - Do not use words found in a dictionary
    - Longer, more complex passwords are better (think passphrases rather than passwords)
    - Do not use the same password for multiple services
    - Use two factor authentication when possible
    - Use a password vault (1Password, LastPass, or Dashlane)
- Phishing
  - This is the act of tricking somebody into revealing information by pretending to be a reputable source. Spear phishing is the most successful technique on the internet today and accounts for roughly 91% of phishing attacks. Here are some things to keep in mind when trying to remain unaffected:
    - Use caution before acting on seemingly random requests via e-mail
    - Only open emails from trusted senders
    - Open e-mails as plain text rather than HTML
    - Do not open or view un-requested attachments
    - Refuse to provide information over the phone regarding bank account status or computer status
- Updating Devices
  - Keeping your devices up to date is an important practice in remaining safe online. This helps prevent your devices from being exploited to the most recent vulnerabilities.
    - Avoid going online with antiquated computers such as Windows XP or Vista machines
    - Verify newer devices are getting updated regularly in order to maintain safety
    - Use security software (Windows Defender, Norton, McAfee, Avast, etc.)
- Public Wi-Fi
  - Locations with public Wi-Fi are convenient for those of us with limited data. Information is generally transmitted in plain text (unencrypted), therefore, we must be diligent in what we do and how we protect our data when connected to these networks.
    - Save sensitive activities (Banking, etc.) for when connected to a more secure network (Home Wi-Fi, Mobile Data network.)
    - Consider a VPN (Virtual Private Network) for encrypting data

It's important to be smart on how we use the internet. We all have our daily routines, if we pay attention to the sites and services we frequently access, we will be better at picking out abnormalities when they occur. Don't let the information here deter you from experiencing the internet, remember knowledge is power. Use this information to make your experience safer and more enjoyable.