CYBER SECURITY AND SAFETY TIPS

By: Mike Smith, MHS Consulting
Email: info@mhsconsulting.net
Main Phone: 215-253-4322

MHS CONSULTING

Screen all phone calls. Set your home phone to lowest number of rings and let all calls go to voice mail. Only answer or return calls to persons you know. If you do answer, do not be afraid to hang up. Never give personal information over the phone.

Do not call. If any number pops up on your computer screen that asks you to call, don't do it. Do not allow a stranger to remotely access your computer.

Lock your devices. Use the security option to lock phones, tablets and computers. Set the screen lock to one to three minutes.

Use strong passwords. Use a different password for each website. It should conform to the website policy. Most require at least 8 characters, upper case, lower case, number and a symbol. Do not save passwords in your web browser.

Password management options. Use a password manager like LastPass or Sticky Password to securely store multiple passwords to multiple websites. You can use a password protected document or spreadsheet. If you must write it down, store it in a safe or locked file cabinet.

Security question answers. When you reply to specific security questions, spell your answer backwards or add a pin number before and/or after you answer. Keep the answer all lower case.

Update Operating System and applications. Apply the latest operating system updates and update applications such as Adobe Flash, Adobe Reader and Java. When updating software always pick advanced and uncheck additional 3rd party or partner software that is being recommended. Do not let software change your existing browser home page and search settings.

Performance enhancement software. Don't install programs that claim they will optimize computer performance.

Type the exact website address (URL). Do not search for a company's support phone number. Go to their exact website to find the proper number. Sometimes the top search engine results are ads and not a direct link to the real company.

When in doubt, throw it out. Clicking on links in emails and social media, like Facebook, is often how bad guys get access to personal information. If an email looks strange, even if you know the person, it's best to delete. You can call the person that it is from to confirm if the link is legitimate.

Wi-Fi in public places. Never trust the Wi-Fi in a public location. Do not perform any banking or financial transactions while on public Wi-Fi.

If you are experiencing issues with security on any of your personal devices, don't hesitate to give us a call and we'll be happy to help.