INTERNET SAFETY CHECKLIST

Courtesy of Coder Scoop, programmers of safe web and mobile apps! https://coderscoop.com

NEVER DO THIS

- ☐ Never open an email attachment without running it through an anti-virus first.
- ☐ Never click on links in emails. Copy them into your browser location bar to see what they really look like! Shun redirected links through bit.ly, goog.gl and similar.
- ☐ Never visit a web site you don't know without first checking it for malware (use Sucuri SiteCheck or similar), even if from Google search results.
- ☐ Never use the same password in more than one place. Hackers know that people do that and will try your social accounts, etc., with your stolen credentials.
- ☐ Never put passwords in plain text in emails, chats or anywhere else. Send them inside encrypted files that only the recipient has the password to open it (give it to them on the phone)
- ☐ Never give sensitive information to callers you don't know who claim to be from your company or a trusted outside firm – call them back through the switchboard of the company, or better still, ask them to walk over. Note that Caller IDs can be easily faked.
- ☐ Never put your personal data on an insecure web form (http instead of https).
- ☐ Avoid giving your credit card or other sensitive information to just any website. Use a PayPal or digital wallet instead so your financial information stays secret.

ALWAYS DO THIS

- ☐ Update your software as soon as there's a new version released. This goes for operating systems, desktop and server software, mobile apps, etc.
- ☐ Make each password unique and totally random, making it as long as allowed. Use a mix of special characters, upper/lowercase combinations and numbers. Store your passwords in a reputable password storage tool. There are also free tools to generate passwords.
- ☐ Enable and use two and even three factor authentication wherever they're offered.
- ☐ Install an anti-virus on all your devices and run them frequently.
- ☐ Always use VPN software when using a public Wi-Fi network.