Internet Security Best Practices

In General:

Avoid Public or Free Wi-Fi:
Attackers often use wireless sniffers to steal information as it is sent over unprotected networks. Also, only check your accounts on devices your trust.

Keep Your Browser Software Up-to-Date:
New patches are often released to fix existing vulnerabilities in browser software. This recommendation doesn't apply solely to browser software – it is critical to keep operating system software and any other software you have up-to-date for the same reason.

Run Anti-Virus Software:
Anti-virus software provides protection by scanning for and removing malicious files on your computer. There are many excellent options for virus protection software (both paid and free), so it is up to you to do a little research and select a program that best fits your needs.

Log Out:
Always remember to log out of important accounts like financial accounts, email or social network sites when you are finished, or if you are going to be away from your computer for an extended period of time. On some websites, simply closing your browser or visiting another website will still leave your account accessible. When you log out, you end your session. This means you will need a username and password to access your account.

Passwords:

Don't Reuse Passwords:
Using the same password for multiple sites only makes it easier for attackers to compromise your sensitive information. Also, never disclose your password to important or private online accounts to anyone.

Use a Password Manager:
Use a password manager to store and create long, cryptic passwords for all of your online accounts. Henssler Financial recommends LastPass, an award-winning password manager that saves your passwords and gives you secure access from every computer and mobile device. The maximum password length the Planning Portal will allow is 20 characters.

If Nothing Else, Use a Passphrase:
While we strongly recommend a password manager, if you do not want to use one, consider using a passphrase instead of a password. A passphrase adds a layer of security because it contains multiple words to create a phrase. An example of a passphrase is hellotomysunshine. For more complexity, you can capitalize each word and swap letters for symbols. Doing so to the first example would yield Hello2My$un$hine. Again, keep in mind, the maximum password length is 20 characters.

Disable Stored Browser Passwords:
Nearly all browsers and many websites in general offer to remember your passwords for future use. Enabling this feature stores your passwords in one location on your computer, making them easier for an attacker to discover if your system gets compromised. If you have this feature enabled, disable it and clear your stored passwords.