HBE Wealth Management LLC

Cybersecurity "Never Ever" List

Never ever will the IRS email, text or call you to initiate a tax bill or refund. The IRS will always contact you via U.S. Postal Service mail. If you are contacted by an alternate method, look up the number for your local IRS office and report it.

Never ever will someone know your computer has a virus. Someone calling and telling you that and offering to fix it is attempting to gain unauthorized access. Popups on your PC with a number to call are also fake. If you think your computer has an issue, physically take it to a business you know to be legitimate.

Never ever write down or re-use the same passwords. Passwords should never be written down – they can easily be lost or stolen. Using the same password multiple times increases the risk of a data breach involving one password leading to other accounts being breached. Consider using a password manager.

Never ever take online quizzes about yourself. These quizzes are mostly designed to gather data about you that could be used to correctly guess your answers to security questions.

Never ever share vacation plans on social media. Doing so alerts others to when you may not be home for an extended time. Also, avoid posting photos of your trip while still on vacation and instead wait until you get back home.

Never ever skip past two-factor authentication when setting up your account for a web site or app. Two-factor authentication is a great way to add an extra level of security and protects you if your password for that account is ever stolen.

Never ever respond to pressure or threats from an email, phone call or text. These are almost always a method of social engineering designed to get you to give someone money or sensitive data. Instead, call the company that the person is claiming to be from at a phone number you know to be legitimate to let them how you were contacted and to confirm it was fraudulent.