Beware of 5 Most Common Social Media Scams!

1. **Hidden URLs**
    a. Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL ("Uniform Resource Locator," the Web address) hides the full location. Clicking on such a link could direct you to your intended site, or one that installs all sorts of malware on your computer.
2. **Phishing Requests**
    a. You may get a message that says something like this: "Somebody just put up these pictures of you drunk at this wild party! Check 'em out here!" If you click on the enclosed link and takes you to your Twitter or Facebook login page, **don't log in**. A hacker can access your password, along with total control of your account. Both the email and landing page were fake. That link you clicked took you to a page that only looked like your intended social site. It's called phishing. To prevent this, make sure your Internet security includes anti-phishing defenses. Many freeware programs don't include this essential protection
3. **Hidden Charges**
    a. You may also be asked to take a quiz or play a game. It may say: "What type of STAR WARS character are you? Find out with our quiz! All of your friends have taken it!" This may sound interesting, but don't enter your info and cell number, as instructed. This will subscribe you to a service that may charge your cell phone bill every month.
4. **Cash Grabs**
    a. Some hackers may be looking for an easy way to get cash. Avoid messages from strangers or friends requesting money. Sometimes hackers can log into your friend's accounts and contact you. You may see something like this: You just received an urgent request from one of your real friends who "lost his wallet on vacation and needs some cash to get home." So, being the helpful person you are, you send some money right away, per his instructions. But there's a problem: Your friend never sent this request. In fact, he isn't even aware of it. His malware-infected computer grabbed all of his contacts and forwarded the bogus email to everyone. Again, think before acting. Call your friend. Inform him of the request and see if it's true. Next, make sure your computer isn't infected as well.
5. **Chain Letters**
    a. You are likely to also see chain letters. It may appear in the form of, "Retweet this and Bill Gates will donate $5 million to charity!" But hold on, let's think about this. Bill Gates already does a lot for charity. Why would he wait for something like this to take action? Answer: He wouldn't. Both the cause and claim are fake. So why would someone post this? Good question. It could be some prankster looking for a laugh, or a spammer needing "friends" to hit up later. Many well-meaning people pass these fake claims onto others.