Security when using social media, especially while sheltering at home

Friday, April 24, 2020

People are using social media today, more than ever. The stay-at-home orders due to Coronavirus are driving people to use their computers, smart phones and tablets more and more, and for longer periods of time. Unfortunately, what comes with that is an increased presence of the internet bad guys; the people out there coming up with ways to scam, hack and grab your personal information and use it for their own gain. The bad guys are reportedly attacking at higher rate since the virus began its destructive track. So it is important to take precautions not only to fend of the virus, but to fend off cyber attacks and hackers.

Here are some of the ways scammers try to get us to act or share our personal information on social media.

- **Fake celebrities**

  We've become so used to seeing what our favorite stars are up to on social media that it might seem natural for them to get in touch to solicit charitable donations, offer backstage passes or profess their gratitude personally. It's not. Social networks swarm with impersonator accounts set up to hoax or fleece fans.

- **Facebook quizzes and surveys**

  They may seem like harmless fun, but the Better Business Bureau and digital-security companies warn that swindlers sometimes use quizzes to pry loose personal data. Launching a quiz app may give its creators permission to pull information from your profile, offering hackers an opening to hijack your online identity. And look out for innocent-sounding queries; you might get a cute note, tweet or post from a friend

asking you to answer a list of seemingly random, harmless questions; Have you ever been in a police car? What was the name of your first dog? Coke or Pepsi? What is your favorite color? Lists like this are actually tools the bad guys use to hack your account. It may be that among the ten questions on the list (that was probably initially circulated by a hacker) just one of those answers is needed for mining your data. So they lull you into a false sense of safety; surely disclosing if I like Coke or Pepsi better can't hurt me. No, but disclosing your high school mascot or year of graduation could give a hacker that last bit of info they need. So be careful what you give away online. Con artists know these are common security questions that banks and financial firms use to protect accounts.

- **"Is that you in this photo/video?"**

  If you get a message like this with a link to purported online evidence of embarrassing behavior, repress your curiosity and hit "delete." Clicking the link takes you to a site that mimics one of the popular social networks and prompts you to log in, a ploy for hackers to get your credentials and access your account. Similarly, scammers have been known to use Facebook's tagging feature to quickly spread malware, via links to supposedly salacious videos.

Other methods to be wary of....

- Posts and ads that offer super low prices on popular name-brand goods or free trials of miraculous health and beauty aids. If a discount or product claim seems too good to be true, it probably is.
- A post that directs you to another website to claim a prize, win a gift card, take a quiz, fill out a survey or see a scandalous video.
- Posts and direct messages that ask for money, even if they appear to be from someone you know; that person's profile may have been hacked or duplicated

One other important thing to know is that protecting your passwords is absolutely crucial. Current recommended guideline suggest that you use a password/phrase of at least 16 characters. The time it takes to hack our information goes up significantly when you use a larger set of characters, but

don’t use random letters as you’ll never remember them. You can replace certain letters with characters or numbers – here are a few examples:

Password Tips

- $ or 5 for S
- 1 or ! for I
- @ for A
- 3 for E
- 9 for G
- 0 for O
- 8 for B

And it is usually required, but definitely recommended to use a mix of upper and lower case characters, along with at least one number and at least one symbol. It is also a good idea to change your password often, to not use the same password in sequence Johndoe1, Johndoe2, etc. and to never keep written passwords with you or in a conspicuous place, like stuck on the inner side, facing out of your phone case, or on your laptop/tablet cover.

And finally, here is a handy list of what to do and what not to do from AARP.

Do's and Don’ts

Do’s

- Do check and regularly update the privacy settings on your social media accounts. Use options to limit access to your posts to people you know and to restrict permissions for apps to access your profile information.
- Do use different passwords for different accounts, and set up two-factor authentication, which ensures that only you can access an account even if someone else gets your password.
- Do think carefully about what you post about yourself and your whereabouts. Hackers can use personal information for identity theft, and a seemingly innocuous vacation photo can signal to criminals that your home is empty.

- Do be wary of strangers who attempt to forge close bonds or romantic relationships on social media, and cut off contact if they start asking for money.

Don'ts

- Don’t include personal information, such as your home address or phone number, in your public profile.
- Don’t accept friend requests from strangers.
- Don’t download apps via links on social media unless you need them and can confirm they come from a trusted source.
- Don’t take social media quizzes or surveys that ask personal questions, even ones that sound innocuous.
- Don’t click on suspicious links, even in posts from people you know — their accounts may have been hijacked. Website safety checkers such as Google Safe Browsing or VirusTotal can tell you if a link carries a phishing or malware risk.
- Don’t log in to Facebook or other social media sites while using a public Wi-Fi network. Many are poorly secured, leaving openings for scammers to intercept personal data associated with your accounts.

Source: Traci Baker, Director, Community Activities & Communications