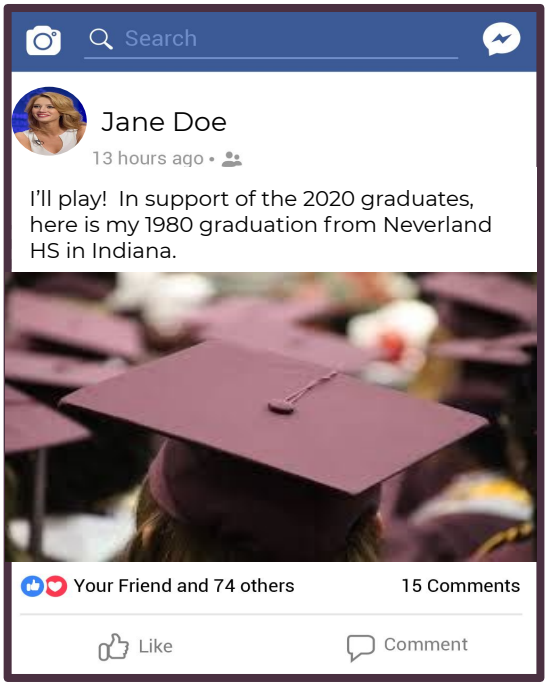
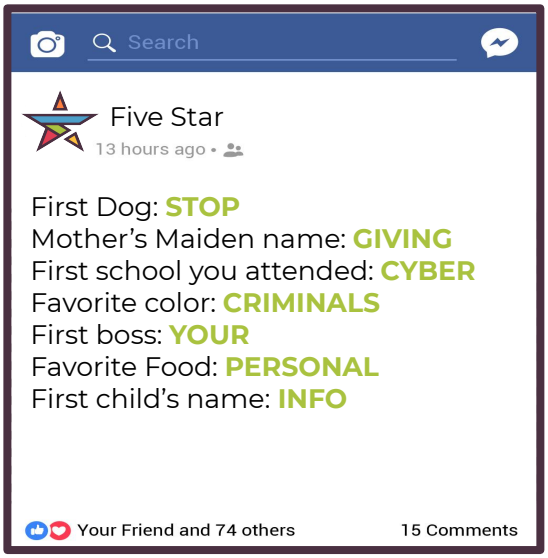
COVID-19 | Cybersecurity & Social Media

During this extended lockdown period, everyone is bound to get a little stir crazy. This can lead to an increase in social media use, including seemingly innocent games/posts where an individual may share personal answers to a list of questions. This is a great time to remind everyone of best practice social media usage.





Source: image: Freepik.com

Five Star would like to caution against providing such information online. Cyber criminals look for ways to hack into accounts and this is a perfect example of using social engineering to do so. Typical questions in games like the one described above are potential security questions and/or hints at your password.

Enable 2FA. Two Factor Authentication requires you to provide a second form of authentication in order to access accounts. For example, approving a sign in from an app or text message code. This is a great way to increase overall account security. All major social media platforms have this as an option in the account's security settings.

Change the privacy of your posts. Cyber criminals look for easy ways to gather information from you. Anything you post publicly puts you at risk. Limit your posts to friends only.

Limit connections. Do you really know this person? It's nice to have friends, but best practice is to make sure you know who you are truly adding to your friend's list.

Limit 3rd party applications. Make sure you know what access you are giving 3rd party applications. Does this application really need access to your camera roll at all times? 3rd party applications are often games you play through social media platforms.

Need more support? Contact Tyler Jones at tjones@five-startech.com