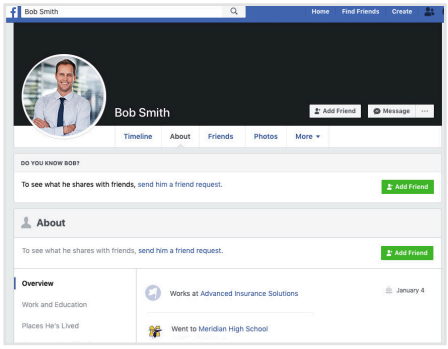
SAFE Tip Sheet
Social Media Security

3.4 billion People now use social media. That's 45% of the total world population. And millions of these users log onto their social media profile every day.



Bob is one such user. He likes to log on and share photos, let friends know what he is up to, and find out what his friends and family are doing.

Bob's profile includes lots of information; his Name, Date of Birth, where he Lives, where he Works, his Interests and Hobbies, Skills, Relationship Status, Telephone Numbers, Email Address, and his Favorite Restaurants - and everyone can see it! ***This is bad. Why?*** Because Bob didn't learn about the Privacy Controls available on his social media sites. He doesn't realize that not only can his friends and family see his profile and posts, but everyone else can see them. *He doesn't realize that in the wrong hands, the hands of a cybercriminal, he could be tricked into giving up much more.*

With his information they could start phishing him for other information, (like his banking credentials), trick him into clicking on malicious links or documents in an email or message, or create a fake account that looks just like his and start tricking all his Contacts as well.

Don't be like Bob!

- Learn about the ***Privacy Controls and Settings*** on each of your social media sites to control who sees your profile and what you post.
- Use ***Multi-Factor Authentication*** whenever available.
- ***Don't post about ongoing or upcoming travel*** or any other schedules that might let bad guys know when you or your family are, and are not, at home.
- ***Photos you post can have information*** as well, like date and time taken, exact location, photographer, or any notes you add to the photo, including tagging with names of your friends and family. Check the Properties of your file to see what is there and remove personal information you don't want to share.

WHAT SHOULD YOU KEEP PRIVATE AND NOT POST?

- Your home address
- Your personal phone numbers
- Your birth date
- Current location
- When you'll be out of town
- Current work-related details (this could be providing non-public information to competitors, or violate NDA's your company has with customers or others)

Don't Take the Bait If:

- ***You are asked to log into a social media site a second time.*** It's a common scam, designed to steal your login information.
- ***You are asked to "Friend" someone you are already friends with.*** It might be a fake-duplicate account trying to trick you.
- ***Your friend posts the results of a fun Quiz*** and wants you to take it as well - your answers could provide valuable information to hackers.
- ***You "Like" or "Favorite" your financial institutions.*** You could be setting yourself up to be a victim of a phishing attack that purports to be from one of these companies telling you they need to verify your username and password for security reasons.

REMEMBER...

What you post online, stays online – think twice before posting that picture you wouldn't want your parents or future employers to see.

Keep personal information personal – the more information you post, the easier it is for a hacker to steal your identity, access your data, or commit other crimes, possibly as you!

July 2019