



Keeping Social Networking, Privacy Settings, and Mobile Apps Secure

Social networking sites like Facebook, LinkedIn, Instagram, or Snapchat or messaging platforms like Slack, WhatsApp, or Skype allow us to share personal updates while communicating with friends and co-workers across the globe. While these convenient technologies keep us connected, are you putting yourself at risk for cyber attackers to watch and learn what you are doing? How should you conduct yourself online? Are you downloading mobile device apps that put you at risk?

Own your security. Here are a few tips to help you leverage these technologies safely and securely to stay protected:

Passwords

Shield yourself and your data. The best way you can protect each of your individual social networking accounts is to implement a strong, unique passphrase for each account. A passphrase is simply a long password made up of a collection of multiple words, making them both easier to type and remember. For example, instead of using 'Password123', an effective passphrase might be 'SummerFootballUnicorn!'. Using a unique passphrase for each account ensures that if one account is hacked, your other accounts remain secure. Can't remember them all? Consider using a password manager.

Poor, easy-to-guess passwords are one of the most common ways cyber attackers can hack into and take over your social networking accounts. Once they're in, they can gain access to your contacts, your private information, photographs, and so on. These security measures can also help protect your information if your devices are lost or stolen.

To further protect yourself, always enable multi-factor verification (sometimes referred to as two-step verification or two-factor authentication) whenever it is available. Multi-factor authentication is when you are granted access only after you have successfully provided two or more pieces of evidence, such as your password AND a unique code generated by your smartphone or texted to you via messaging.

Enable Privacy

Whenever you choose to post information about yourself online, it is good practice to assume any information you post could eventually become public. Avoid communicating about sensitive or private details about yourself. It is also wise to avoid posting any images of yourself that you wouldn't want someone like your parent or employer to see.

When you register for a social networking site, your first step should be to enable and customize your privacy controls. While it may help, keep in mind that these controls can be confusing, they might change often, and they may not fully protect your information.

Don't assume that once you've established these privacy settings that your account is fully protected. Having the most up-to-date security software, web browser, operating system and apps is the best defense against viruses, malware and other online cyber threats.

Anything you Post Could be Used Against You

The more information you post about your personal life, the easier it is for a cyber attacker to customize an attack against you. For example, if you post extensive information about your family, the hobbies you enjoy, or your upcoming vacation or work trip, a cyber attacker could harvest all of those specific details and create a phishing email or phone call that specifically targets you.

If you were to post about your favorite pastime, such as baking, the cyber attacker could craft a phishing email with a special promotion for a new mixing bowl set. In this email, the attacker could include an attachment that has a 50% off coupon for your favorite baking supply brand. What you don't realize is the attachment included in that email is actually infected. When you open the attachment to print it out, it silently infects your computer, giving the cyber attacker total control of your system. Keep this in mind when you get an email about a fantastic vacation similar to the one you just took, or a fantastic deal concerning one of your favorite hobbies. If it seems too good to be true, it probably is.

Be an Advocate

Be aware. Keep track what your friends and coworkers within your network post about you. It isn't rude to ask them to be considerate of your privacy. If you feel as though something they post is inappropriate or you feel as though it shares too much information about yourself, kindly ask them to remove the content. You could also report it to the website's abuse department, if you'd prefer.

In return, practice the same level of consideration of what you post about your friends and coworkers on your social networking sites. It would be good practice to ask them if you have their permission to post a picture or share details you have of them.

Third-Party Applications

Your mobile devices are just as vulnerable as your PC or laptop. As much as you want to trust an app, take a moment to read the fine print. Many social networking sites or mobile device apps also support third-party applications. Inspect the details when downloading an app or registering for a new network. Only install applications from trusted sources and only install the apps you truly think you need.

Get into the habit of checking the ratings, reviews, and permissions of any app before you choose to install it. It could be a big red flag if an app is very new, has few or negative reviews, or very few downloads. It would be in your best interest to not install it.

Often times, you might download an app for a specific, short-term purpose, such as planning a vacation, or a home renovation. Conduct regular audits on your apps. If you no longer need an app, uninstall it or disable its access to your social networking profile, as it could still be collecting data.

Be Suspicious

Much like email phishing attacks, cyber attackers may attempt to trick you on your own social networking sites. A common attack method is when a cyber attacker hacks into a friend's social networking account and pretends to be that friend online. They may send you an urgent request, such as being mugged or stranded while on vacation and needing money sent right away.

If you receive any odd or suspicious messages online from a friend, proceed with caution and be careful how you respond. Do not reply directly via their social media account, as you will be communicating directly with that cyber attacker. Instead, call your friend on the phone to confirm if he or she truly posted the message and needs your help.