Cybersecurity And Your Social Media Accounts

Whether you are showing off a meal you are about to eat, creeping your frenemies or staying in touch with family and actual friends, social media has got it all.

However, as is often the case with anything free, there are drawbacks.

Throughout my years of experience in the world of cybersecurity and digital forensics, I have seen how social engineering is the most effective way criminals are able to breach organizations and steal data. These attacks are able to take place because cybercriminals search for personal information on social media accounts that they can then exploit.

With that said, here are some tips to help keep you, your colleagues and your loved ones safe on social media:

1. Many fraudsters love to start by making their way onto our friend lists. With that in mind, make sure to verify your friend and follower requests before accepting any of them.

2. When you allow access via add-ons like games from third-party vendors through your chosen social media platform, make sure you understand what you are agreeing to, and what information of yours and your friends the company will now be able to get their hands on.

3. Make sure to customize your privacy settings! You want to avoid having all of your information be seen by the general public. Keep certain things for your friends and family only.

4. Take special precautions before you click on a link, attachment, download, email or anything else sent to you — especially when it's sent to you via social media. Even if it is seemingly from someone you know, they could have had their account breached.

5. Many of the social media platforms we use have pretty good security tips specific to their respective sites. Spend some time reading those specific tips before you get started using those platforms.

6. It’s not a good idea to reuse passwords or use the same password for all of your favorite sites. If your password gets leaked through a company breach, then a cybercriminal can use that to breach all of your accounts that use the same password.

7. Remember, it is possible to be fired from your job for posting something you shouldn’t. Be mindful of what you post on social media.

8. Make sure to turn off auto-geotagging. Auto-geotagging is when your GPS information is automatically tagged with your status updates, thus giving a hacker a Google Maps indication of exactly where you are at the time of your post. There are so many reasons this is a bad idea that I could write another article just on that topic alone.

9. Don’t post about when you are going on vacation.

10. Remember what goes online can very well stay online forever, even if you think you posted it to a private site. This could come back to haunt you through a hack, breach or privacy policy change. If you delete a picture you are embarrassed about from your account, it is most likely still sitting on a server somewhere. Alternatively, someone could have downloaded or taken a screenshot of it before you took it down.

One last thing to remember about your personal information and social media: Even if your account isn’t hacked or researched by a cybercriminal, your personal information can still be compromised. By accepting the terms of your chosen social media platform, you’ve most likely given the rights to that company to do what it would like with your personal information. Always remember that when you are not paying for something, you are not the customer — you are the product being sold.

Your personal information and the information of your colleagues and loved ones is worth a lot of money to cybercriminals. So remember to employ these tips and be careful about what you post on your profiles.

By Danny Pehar