Zoya Qazi

4/24/25

MIS 4596 - Spring 2025

 Keeping Your Social Media Identity Safe

In the era of digital communication, social media has taken center stage in our lives. Instagram, Snapchat, and TikTok allow us to share everything, from beautiful breakfast pictures to graduation posts, but at what price? Cybercriminals are always keeping an eye on us behind the hashtags and filters, waiting to take advantage of our digital traces. Social media is a treasure trove of personal information, as demonstrated by the cybersecurity case studies and experiments in this course. This essay examines the increasing dangers of social media, connects them to actual cyberthreats like social engineering, ransomware, and password cracking, and explains how to regain control of your online persona.

Social media is risky because it is intentionally public. Through friend requests, tagged posts, or compromised apps, information can even be leaked from private accounts. In order to obtain access, hackers employ social engineering, which involves manipulating people rather than disrupting systems. Attackers may pose as a brand and send phishing URLs or phony gifts that appear authentic, as demonstrated in Lab 9: Social Engineering. They can enter your account with only a single click.

Your profile may be used to gather even innocuous information, such as the name of your pet or your favorite color, which are frequently used in security questions. Cybercriminals can use this information to create customized phishing emails, circumvent security checks, and guess passwords.Changing your password habits is one of the simplest methods to increase your security. Using the same weak password for several accounts is a big mistake, as we discussed in the Password Security reading. A hacker can access all websites if they manage to gain access to only one (for example, through a data breach). Strong passwords should be unique for each platform, contain a minimum of 12 characters, and combine letters, numbers, and symbols. Always use two-factor authentication (2FA) while creating passwords. Our studies and discussions of real-world cases stressed this point: 2FA means that even if a hacker manages to figure out your password, they will still require a second verification step, such as a code texted to your phone. The majority of account takeovers are prevented by this easy-to-use technology.

Suppose someone gains access to your account. That can be disastrous in addition to being embarrassing. Hackers can spread software, pose as you, or even start ransomware attacks using social media accounts they have hijacked. As discussed in the reading summary on ransomware, hackers encrypt data and demand payment to unlock it. Ransomware typically targets corporations, but it can also affect individuals, particularly those with a big following or influence.

Our vulnerability exploitation laboratories demonstrated the speed at which an attacker can proceed after they have gained access to a system. They could send phishing links to friends and followers, change additional passwords, or pose as you if they have access to your email or chats.

Cybersecurity extends beyond the confines of a computer. Protecting your digital identity, particularly on social media, greatly depends on physical security. Leaving your phone unlocked in public or leaving your laptop in a coffee shop can easily lead to a breach, even if it may not appear related. Threats like shoulder surfing—where someone watches you input passwords—and physical device theft are genuine dangers, as was covered in our class's Physical Security short. Someone might see your private messages, Instagram, Snapchats, and even reset the passwords to other accounts if they manage to get their hands on your unlocked phone. This serves as a reminder that security entails more than simply passwords and apps. The larger picture of remaining secure in both digital and physical settings includes avoiding unprotected public charging stations, keeping gadgets close to hand, and locking your phone with a PIN or Face ID.

The South Carolina Department of Revenue (SC DOR) hack, which we discussed in class, was one of the most obvious real-world examples of how minor errors may have significant repercussions. Millions of records were compromised in this huge breach, which was caused by a single mistaken click in a phishing email. It brought to light a fact that is true for everyone, not only government workers: being a cybersecurity expert is not a prerequisite for being a target. Hackers take advantage of people's tendency to underestimate the consequences of disclosing little information or clicking on dubious links. This could appear on social media as a direct message offering a reward or cooperation, or it could be a link from a phony friend account. The SC DOR episode demonstrates that the same strategies that are employed to undermine large institutions are also applied to people on a daily basis. Being mindful and cautious is your best line of defense.

Our labs gave us practical knowledge on how attackers identify and take advantage of vulnerabilities throughout the semester. We studied vulnerability scanning—tools and methods for finding security holes in systems—in Lab 6. Hackers examine social media accounts for flaws like re-used passwords, unpatched programs, and publicly viewable personal information, much way they can scan servers and websites for vulnerabilities. By showing how attackers take advantage of those vulnerabilities after discovering them, Lab 7 went one step further. These actions were a reflection of what actually occurs when an account is compromised. This was further supported by our Penetration Testing Report, which demonstrated how a single weakness, whether human or digital, can be exploited to obtain unauthorized access and steal confidential data. These labs highlighted the importance of protection by demonstrating the step-by-step reality of what a hacker could do if they gained access to our digital lives.

Being confident and in charge is more essential than being paranoid when it comes to protecting your online persona. The necessity of creating strong, one-of-a-kind passwords and utilizing two-factor authentication to prevent unwanted access are two of the most significant lessons learned from our training. Links in direct messages and comments should also be carefully considered because many phishing attempts pass as promotions or cordial remarks. Another easy yet effective way to manage who can contact you and who can view your postings is to change your social media privacy settings. Updating your programs on a regular basis helps address known vulnerabilities, and being careful about what you post online can stop someone from exploiting it against you. You can enjoy yourself online without worrying about security; it just means that you have complete control over your accounts, content, and identity.

Nowadays, cybersecurity is a way of life rather than merely a technical concern. It's crucial to take your online safety seriously in a world where your online persona might be just as genuine as your offline one. Everything we've covered this semester, whether it's about safeguarding your social media accounts, creating secure passwords, or learning from actual security breaches like Equifax or SC DOR, speaks to the same conclusion: it's your responsibility to be safe online. You should protect your privacy, your data, and your identity. You won't have to be afraid of threats if you have the correct resources, awareness, and attitude. You may express yourself on social media, and cybersecurity is the way to ensure that it remains yours. Be clever, be cute, and keep your peace both online and offline.

Citations

Cybersecurity & Infrastructure Security Agency. (n.d.). *Social media cybersecurity tips*. CISA. Retrieved April 25, 2025, from <https://www.cisa.gov/news-events/news/social-media-cybersecurity-tips>

Federal Trade Commission. (n.d.). *The Equifax data breach*. Retrieved April 25, 2025, from https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

BBC. (2018, August 22). *How NotPetya crippled Maersk, the world’s largest shipping firm*. BBC News.<https://www.bbc.com/news/technology-41319683>

NortonLifeLock. (n.d.). *What is social engineering?* Norton. Retrieved April 25, 2025, from <https://us.norton.com/blog/emerging-threats/what-is-social-engineering>

South Carolina Department of Revenue. (2013). *South Carolina Department of Revenue data breach report*. South Carolina Government.