Module 2: Activity 2

Harsh Siddhapura

Ira A. Fulton Schools of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Dr. Jim Helm, Prof. Upakar Bhatta

August 25, 2023

“Credit to Bill Fitzgerald and funnymonkey.com/2017/privacy-and-security-exercise”

“Do this exercise with your phone, tablet, and/or any computer you use regularly. Imagine that someone has accessed your device and can log in and access all information on the device. Answer each of the following questions in one to two paragraph explanations. You will be evaluated on the details of your answer.”

“As you do this exercise, be sure to look at all apps (on a phone or tablet), online accounts accessible via a web browser, address books, and ways that any of this information could be cross referenced or combined”

1. **“If they were a thief, what information could they access about you?”**

   The information that the thief could potentially retrieve are:

   - Monetary details:Information related to financial transactions and funds.
   - Digital profiles:Online accounts on the internet, often associated with social media, email, or other digital platforms.
   - Personal images and videos:Visual material that poses a threat to an individual's privacy.
   - Records and data of the person:Information pertaining to personal or professional matters that could be advantageous for a thief to obtain and exploit for their own objectives.
   - Personal communication:This information could be used to pressure the individual into meeting the thief's requests or exploiting their weaknesses.

2. **“If they were a blackmailer, what information could they access about you?”**

   If the intent of the individual aiming to blackmail, they might seek:

   - Credit card information
   - Social media passwords
   - Professional work details
   - Private photos
   - Networth

3. **“What information could they access about your friends, family, or professional contacts?”**

- Unauthorized access might reveal my contacts list, which contains names, phone numbers, email addresses, and potentially links to social media profiles.
- This information could expose details about my friends, family members, and the nature of our relationships.
- The contacts list also includes contact information for colleagues, clients, and other professional contacts I've interacted with.
- Exploiting this data could lead to potential identity theft risks, as the exposed information might be misused for fraudulent activities.
- Additionally, the accessed contacts could become targets for personalized phishing attacks, utilizing the gathered information for an identity theft.

4. **“What information could be accessed about people you "know" via social media accounts?”**

   Illegitimate access to my social media accounts might grant entry to my roster of friends, affiliations, and online engagements. This data could potentially be cross-referenced to deduce information about my social circles and interpersonal connections. For instance, analyzing the frequency of my interactions could facilitate the identification of close friends and associates. Furthermore, particulars about planned events or locations I've marked as visited could be exploited to monitor my whereabouts.

5. **“What steps can you take to protect this information?”**

   There are several ways to protect our data even after our device is stolen. Firstly, we can enable two factor authentication (2FA) for online or mobile banking. This will add the extra layer of security as the authorization code, or the push notifications require another device to authenticate and grant access to the user. Secondly, online ordering applications such as amazon, Instacart, Uber, Lyft and many more where we save our credit card information are vulnerable to be manipulated.

Instead of saving our card details, we can manually enter every time so that even after the theft it doesn't harm. Thirdly, professional information such as emails, team chat or slack can be password or pin protected. We can also enable face id detection in order to open these applications. This will prevent thieves from accessing these applications as it requires biological traits to authenticate.

However, there is little information which can be included such as personal chats, photos, daily schedules, relatives' information, important notes which may include social security number as well. Although we must take protective measures such as keeping it in a secure vault. Another way would be using app lock for each application which contains confidential data.

6. **"Assuming that someone you know has comparable information about you, what steps would you want them to take?"**

If I know someone who has a handful of details about me, I will want that person to keep that information as secure as possible. This can be achieved in several ways. Firstly, if the person knows any financial information, such as mobile banking credentials, or credit card information, I will make sure the person enables 2FA so that I can receive the authorization code or push notification before any valid transactions. That information will work like a biological trait that will only be known to me. Secondly, if the person is using any of the applications that I use for my personal use,

I will make sure that the person keeps that application safe from vulnerabilities using app locks and pin protected software. In an unlikely event, even if the phone were accessible to a thief, the application data wouldn't be compromised. Thirdly, we can use the person to be vigilant about phishing messages. If the person unknowingly clicks on any malicious links, our data can be opened up. Additionally, we can ask the person to use VPN so that the network can be secure.

Nevertheless, data is always prone to manipulation if it is not secure. Sometimes, after taking all the preventative measures, the data can get transferred and altered. If the person has some media files that include photos and videos about me, I will advise the person that they should be kept in a nested hierarchical manner so that it is not easily available. Also, it would be better if the person kept that in the cloud and provided access only to me so that no one else could view it.

7. **"Are there differences between the steps you could take, and the steps you would want someone else to take? What accounts for those differences?"**

   In addition to enabling 2FA in sensitive applications, not saving confidential data inside our mobile phones and keeping PINs strictly confidential, the avenues of compromise when a malicious actor has the physical device in hand are inexhaustible. For example, recommended security practice is that one should not recycle and/or reuse passwords.

   We interact with approximately 6 applications a day, (Canvas, banking app, PayPal, Cash App, OneDrive, Google accounts, etc.), which means one has to memorize 6 separate passwords daily. To reduce mental strain, we keep a text file of all the passwords on our phone, which, if the device is stolen, is now available to the attacker.

   So, with all this considered, it is rather safer to have separate devices for various functions, e.g., school/work, banking, and general web surfing. That way, chances of reusing that weak Amazon password on our online banking while signing into the latter over an unsafe wireless hotspot at Starbucks are eliminated.

8. **"When it comes to protecting information, we are connected. At some level, we are as private and secure as our least private and secure friend."**

   The above statement is reasonable. In addition to segregating devices based on work, play and all in-between, it is safe that you do not share with anyone anything you would not want to see compromised. PINs, passwords, no matter how complex, will not hold if 4 people will know about them, or we use them across various platforms.

Discretion, common sense and maintaining zero trust are key to protecting information - as we do when traveling in unfamiliar places. We also have the responsibility of teaching those closest to us the importance of embracing the three qualities in our digital lives.

“Write a summary that is at least 500 words and three paragraphs discussing your results and what you learned from this activity.”

In the undertaken privacy and security exercise, we delved into the potential vulnerabilities of our personal devices and online presence, envisioning a scenario where an unauthorized individual gains access to our information. Throughout the exercise, we meticulously assessed the sensitive data stored on our phone, tablet, and computer. Various categories of information were evaluated, including monetary details, digital profiles, personal images and videos, and personal communication. This activity shed light on the extent to which our lives are intertwined with digital platforms and the potential risks associated with unauthorized access.

The exercise also prompted us to consider potential threats, contemplating situations where an attacker could act as either a thief or a blackmailer. In the context of theft, the focus was on valuable information such as financial details, digital profiles, and personal communication. Shifting to the perspective of a blackmailer, the exercise highlighted information that could be exploited to manipulate or pressure the victim, encompassing credit card details, private photos, and professional work specifics. This phase of the exercise emphasized the diverse ways in which compromised information can be turned against an individual (Wolff, J., 2017).

To counteract these threats, we familiarize ourselves with a range of security measures that can be implemented. A crucial strategy identified was the adoption of two-factor authentication (2FA) for sensitive accounts, adding an additional layer of security. Additionally, the exercise underscored the importance of prudence when saving financial information on online ordering platforms and employing password or PIN protection for professional communication channels. The significance of encryption and secure vaults for safeguarding sensitive files was also highlighted, along with the recommendation to employ app locks for applications housing confidential data.

The exercise also led us to reflect on the responsibilities of individuals close to us who may possess comparable information. Recognizing that someone in our circle might have access to similar data, we learned that mutual vigilance and collaborative efforts are integral. Encouraging them to adopt similar security practices, such as using 2FA, employing app locks, and exercising caution against phishing attempts, can collectively contribute to establishing a more secure environment. The exercise reinforced the notion that our level of privacy and security is akin to that of our least private and secure connection, thereby stressing the significance of imparting education and cultivating a culture of security among our friends and family (Gupte, P., 2019).

In conclusion, the privacy and security exercise provided us with invaluable insights into the potential vulnerabilities within our digital lives and the proactive measures we can take to mitigate risks. The exercise illuminated the multifaceted approach required for safeguarding our information, encompassing technological safeguards, responsible information management, and education. By meticulously evaluating the sensitivity of the data we handle and share, and by proactively integrating security measures, we can significantly bolster our privacy and minimize the potential repercussions of unauthorized access or exploitation. This exercise served as a reminder that safeguarding our information is a collective endeavor necessitating awareness, diligence, and collaborative action, particularly in our interconnected digital landscape.

References

Gupte, P. (2019). Attacking the attacker: Analyzing the legality of hacking back. LinkedIn. https://www.linkedin.com/pulse/attacking-attacker-analyzing-legality-hacking-ba-pranav-gupte

Wolff, J. (2017, July 14). When companies get hacked, should they be allowed to hack back? The Atlantic. https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/