CS7NS5 – Security and Privacy
Assignment 2 – Security and Privacy Incident during the course

By: Pallavit Aggarwal (MSc Intelligent Systems 2022-2023)
Email: aggarwpa@tcd.ie

Having studied the course material, I have come to understand that there are various degrees of security and privacy. While achieving strict security and privacy is the ultimate goal, numerous techniques, covert or indirect methods exist that can undermine security and compromise privacy. The extent to which an individual is willing or motivated to break and work around security protocols can vary significantly.

I did not attempt to explore or discover any gaps in the security or privacy of the college infrastructure or its assets. However, I experienced two significant incidents that made me more aware of the security and privacy aspects of systems:

- The first incident I would like to highlight is when my TCD account (managed by a Microsoft vendor) got locked due to a geolocation-based access control, or "geofencing." I was using a VPN to access apps that I have subscribed to, which only work in my home country. When I tried logging into my account through the VPN, my account was immediately locked. I had to contact the TCD helpdesk to get my account unlocked, which I found to be a useful feature. It made me realize that even account credentials are highly monitored, and there is more than the default security layer behind these accounts.

- The second significant incident I encountered was a scam targeting individuals in housing and renting groups in Dublin. The scammers were probably part of a common group and messaging everyone. They sent me a tempting message, claiming that if I signed in and completed a survey, I would receive a cash reward. The first major security red flag was that the website used the "http" protocol instead of "https." I proceeded with the process to see how it would unfold, and the site asked for a username and password. A common mistake people make is using the same password for different official accounts, which could expose them to hackers or attackers. I used "u$ernam3" and "passwo0rd" as my credentials and provided a temporary email address. After landing on the main page, I received an immediate response from the scammer, making me wonder if any of my other data was being shared. I opened the network tab on Chrome by pressing F12 and checked the XHR calls, GET/POST requests, and the types of headers and data being shared. I noticed that the website was making a call every five seconds, sending my IP address and mouse coordinates on the screen. The scammer then asked me to create a Bitcoin account or use an existing one and connect it to the portal to receive my cash payment. Although I used 2FA with Google Authenticator to access my account, I knew that providing my Bitcoin address or any other detail would only allow the scammer to learn more about me. I tried deleting my account, but I couldn't, so I logged out and blocked the scammer.
  I could have explored more of the website and the API calls it was making to find out more about the scammers, but since it wouldn't have amounted to much, I simply didn't go that route.

This incident made me realize how scammers use a social engineering technique to lure victims into providing personal information and potentially gaining access to their financial accounts (i.e., Bitcoin). While traditional phishing attacks often involve fraudulent emails that appear to be from a trusted source, this incident demonstrates that phishing can also occur on social media platforms, forums, and other online communication channels.

The following were the red flags that I was able to identify:

Unencrypted website: The website used an "http" protocol instead of "https," which means the communication between the user and the website is not encrypted. This makes it easier for hackers to intercept the data transmitted between the user and the website.

Credential harvesting: By asking for a username and password, the scammers attempted to collect credentials that could be used to access other accounts, especially if the victim uses the same login details for multiple sites.

Social engineering: The scammers employed social engineering techniques to manipulate victims into divulging sensitive information. They created a sense of urgency and reward to persuade the victim to provide personal information and potentially expose their financial accounts.

Data collection without consent: The website was collecting the victim's IP address and mouse coordinates without their knowledge or consent. This information could be used to track the victim's online activity or for other nefarious purposes.

Lack of proper account deletion: The fact that the victim could not delete their account indicates a lack of privacy controls, allowing the scammers to retain any collected information indefinitely.

In the context of a college environment, it is vital to implement comprehensive security and privacy policies, incorporating robust measures such as geolocation-based access control, encryption, and multi-factor authentication. Educating students, faculty, and staff about potential risks, including phishing attempts, social engineering tactics, and credential harvesting, is essential for fostering a culture of security awareness and reducing the likelihood of successful cyberattacks.

However, individuals must take personal responsibility for their digital safety and exercise caution when navigating the online landscape. This includes using strong, unique passwords, verifying the authenticity of websites and online communications, and being vigilant when interacting with unfamiliar online entities.

Security and privacy play a crucial role in preserving the integrity of educational institutions and safeguarding the personal information of students, staff, and faculty members. The incidents I experienced emphasize the need for a multi-layered approach to security, incorporating both proactive measures and user education to protect individuals from cyber threats and privacy violations.

Ultimately, achieving absolute security and privacy may be an elusive goal, but by continuously adapting to the ever-changing threat landscape and adopting best practices, we can minimize risks and create a safer digital experience for all.