Cyber Security: Mobile Security 101

The website advice held the continuation of their cyber security webinar series via facebook live to tackle about mobile security. As everyone today uses their mobile phone, this webinar tackles how essential that we safeguard the information while we are accessing internet using our device and what are the thing we should do to secure our information to prevent the mobile threats.

The webinar started with questions about our mobile security such as what kind of screen lock I use, how often I update my phone, do I read terms and agreements of every application I install, and what will I do when my phone got stolen. These questions allow me to reflect how secure my mobile is.

Moving to what is mobile security; it is the practice of defending mobile device from any source of cyber-attacks that can threaten user's privacy, network login credentials, finances, and safety. On the quarter 2 of 2019, the Philippines ranked 5th as most attacked online worldwide, and mobile devices today account for more than 60 percent of digital fraud. And as the mobile device usage increases, it is important that we protect our information from threats: web-based threats, network threats (connecting to unsecure network like Wi-Fi and Bluetooth), app-based threats, and physical threats.

After explaining what is mobile security and threats, the speaker then shared steps to protect our mobile devices. First, create a screen lock as it is the first line of defense in securing the mobile device. Second is avoiding public Wi-Fi because it does not have encryption and is very dangerous especially if a hacker is connected to it. Some of the public Wi-Fi dangers give are network snooping, man in the middle networks, and malware networks. If using pubic Wi-Fi can't be avoided, then it is better to limit the internet activity and avoid checking emails or mobile banking and likes. Third, always update the phone because it is necessary for security purposes. Outdated software and system can risk our phone such as ransom wares, malwares, and data breach. Fourth, delete the applications that are unused and unnecessary anymore. Fifth, download only from trusted sources and evaluate its resources. Sixth is check app permissions especially if it unnecessarily ask access to gallery, contacts or location. Seventh step is to set the privacy setting. By setting it, we control what application will be using location, camera and the likes. In privacy setting, files must be encrypted, disable auto-fill, disable screen notifications, and disable location tracking. Eighth, installing an antivirus to detect malware, to easily locate device when lost, and wipe out information when lost. Ninth, do not click unknown links, messages, or email because it is highly a form of phishing. Lastly, remote lock the phone in case of lost or theft, this will automatically lock the phone when it is lost and will show a message to contact you. Aside from the steps, the speaker added that it is important to find a private place to make calls that might need important data.

The webinar provides useful information and gave insightful tips to prevent being a victim of cyber-attacks, thus, it is important that the steps mentioned above should be exercise.