**LONG QUIZ**

1. What advice will you give to the following individuals on how they can secure their social media accounts free from threats that they may encounter:
   * **8-year-old younger brother**
     + Avoid visiting any strange websites because threats are typically found there. Also don’t open any links that are typically found on the inbox of the social media.
   * **Housemaid / Yaya**
     + Never trust anything you read online. The majority of fraudsters on the internet target young individuals because they are aware that at this age, people are more likely to need money.
   * **75-year-old Lolo or Lola**
     + Don't click on any shady links that have been posted or provided to you. The threats typically target elderly people since they typically have limited online knowledge, also avoid someone who are texting you that they’re your relatives, because this is the usual scam for the elderly.
2. Give at least three Social Engineering attacks and give some tips on how to avoid these.
   * **Phishing** – Typically, a text message or email with an urgent notification about your accounts is sent to force you to log in to a false website that looks almost exactly like the real thing besides the only differences of it is the domain address itself.
     + It can be avoided by not opening any attachment on the message that are being sent to you
     + If you feel wary check your personal accounts in order to prove, also contact the provider of your sensitive accounts.
     + Check the domain address of the real link of the website.
   * **Malware** – When installed, it typically originates from a software pirated attachment or email and can steal important data from your machine, also its relevant when downloading illegitimate or counterfeit applications towards the system.
     + Check the software you are installing on your computer to avoid this threat.
     + Download your software through the trusted websites only.
     + Do not download any link that advertise free download even if you know that, the software you’re downloading has a subscription fee.
   * **Baiting** – Typically from an advertisement that displays deals, gifts, and special offers that a user is powerless to ignore. Sensitive information from a user's attack may also be retained.
     + First that many knows is the ‘Think Before You Click’
     + Too good to be true, there’s no such thing as free see the official of that product to see if it’s real.
     + Getting your information such as debit or credit card in order to avail the free product that they advertise.
3. If you become a network security officer someday, what will you consider in establishing a safe, efficient, and effective network for your company?
   * Establishing a static IP address throughout the company.
   * Disable piracy website, also porn websites throughout the company by establishing reverse engineering on the computer server that connected through lan port.
   * Avoid using pirated software, always use legitimate products.
   * Organize the dos and don’ts in the workforce of the company.
   * Use antivirus in the computer system
4. If the Philippines will adopt a specific Cyber security law from the other country what do you think is feasible and why?
   * **USA’s Cybersecurity Information Sharing Act of 2015 (CISA)**
     + It’s law in the United States of America that will allow United States government agencies and non-government entities to share information with each other as they investigate cyberattacks. Sharing is voluntary for participating organizations outside the government. This law will be perfectly suited on our country because our Government right now lacks on the transparency of data in its indigence, that’s why with this adopting law, it will be beneficial to us, in order know and help with such cases, and the most important thing is that it will be not one-sided investigation which results to greater goods, due to we know that lack of transparency means higher chance of corruption throughout the entire country.