Software Development Unit 3, 1.2

Anna Legaspi

# I can explain what risks there may be in using collaborative technologies and how to keep them to a minimum

## Phishing

Phishing is a cybercrime where cybercriminals send a message via email, text or other social communication app. They pretend to be a legitimate business and try to obtain personal information from the potential victim. Some emails feel fake especially when the email is poorly formatted and this is a bit easier to detect. However, cyber criminals are getting cleverer and more elusive nowadays and there are many victims worldwide that fall prey. Some emails have malicious links that download malware or ransomware into the device. Since these cyber criminals are getting better, the best way is to be cautious when opening emails, especially those that look suspicious. Check for spelling mistakes or anything that may appear out of place. If in doubt, it’s best to contact the company directly instead of clicking the links within the message.

## Malware attacks

One of the intentions of phishing is the installation of malware in the victim’s devices. There are a variety of malware with different purposes such as Spyware, Adware, Worms and Viruses. Spyware obtain credentials for online banking and personal data by copying the keystrokes of the user. Once personal and financial data is collected, they can either sell the data other criminals or use it for their own profit. Adware is another example, where online activity is tracked by the malware and it chooses what type of ads to present to the user.

## Identity theft

If a malware attack is successful, some cybercriminals can use personal information for their own personal gain. For example, the cybercriminal can open a bank account under another person’s name with the purpose of money laundering. Others who are struggling to get credit can pretend to be someone else so they can borrow money from creditors. Overall, the best way to avoid identity theft is to make sure that personal information isn’t posted online and relevant software is installed in their devices to avoid potential malware attacks.

## Data loss / breach

Another type of malware is ransomware. Some criminals attempt to install ransomware where the malware hijacks the whole operating system, rendering it unusable. The cybercriminal would then demand a large amount of money to remove the malware. If the victim refuses to cooperate, they will threaten to delete all the data or even sell the data to other cybercriminals. There have been many malware attacks in history and has cost billions in losses around the world.

## Remote access

There is malware that allow remote access from the cybercriminal to the victim’s device. Sometimes the cybercriminal would call the victim, pretending to be from a legitimate company and pretend that their desktop is at risk. The criminals then offer to resolve the non-existent problem and try to obtain remote access. During this process, they steal all of the victim’s personal information or even install more malware into their OS.

To avoid all the issues stated above, it is best to install an anti-virus and anti-malware software in devices. I personally use Bitdefender which offers robust protection such as Anti-virus, Advance threat defense, Firewall, Ransomware remediation and even Anti-spam. Also, always be vigilant and cautious before clicking a link. If the message is suspicious, it probably is. The best thing is to contact the company directly using their official communication channels.