# **Additional Problem**

With the internet being around for quite some time already, identity theft is nothing new. New and better technology has allowed hackers and online criminals to find new ways to commit these crimes. Online identity theft is when someone steals your identity by gaining access to your personally identifiable information to commit fraud. These malicious hackers could steal personal information such as your Social Security number, bank account number or your passwords. When we share personal info online, that information might risk falling onto the wrong hands. These perpetrators use different methods to commit identity theft. Such methods are: phishing, pharming, malicious software and unsecured websites. Phishing occurs when cybercriminals send emails purporting to be from a financial institution or other trusted organization, trying to trick you into opening attachments or clicking on links and providing your PII. Ignore unsolicited emails and online requests for information. If you want to visit, say, your bank’s website to provide information, type in the URL rather than clicking on an emailed link. Pharming occurs when your browser, compromised by a virus, is hijacked without your knowledge. You type a legitimate website URL into the address bar, but you’re redirected to a fake site that looks legitimate. There, cybercriminals are able to collect any PII you may type into the website. Malicious software is when a hacker tricks you into downloading a malware that does damage to your computer once downloaded. Once attacked, the malware reveals and sends your private information to the hacker. Some websites online are not secured. When a person accesses one of these unsecured websites, they are at risk of getting their information stolen. To know if a website is unsecured or not, Make sure you use only official, secure websites. Websites with the “https:” prefix are safe while other prefixes are unsecured.