COMP-2057 Assignment Six
Ryan Lebeau

“Vacation Fraud Without The Vacation”

This is an emerging email scam that targets your family and friends. Firstly, the scammer hacks into your email and then they will send an email to all your personal contacts. This email contains a plea for help since you have been stranded on your vacation and all of your belongings have been stolen. They can also embed malware into the email to continue this chain of email frauds throughout your entire contact list. The best defense against this fraud is to have a very secure email password and avoid clicking links/opening emails from unknown addresses. Also, being vocal to your contacts that your email has been compromised and you are safe and sound at home. If you have fallen victim to this scam there is not much you can do, since money being wired is nearly impossible to track. Just make sure to spread the word about these attacks to hopefully prevent others becoming prey as well.

“Ransomware: how hackers can hold your files hostage”

Ransomware is a common scam that happens across the globe everyday. You cna pick up the malware from clicking popup ads, downloading malware unknowingly, or even email attachments. Once your computer is infected it will encrypt your files (or more commonly relocate all personal files to a single encrypted folder) and provide you with a payment option to have your files decrypted for you. Preventing this can be as simple as having a strong up to date antimalware on your system. If you do become a victim of a ransomware attack you are best to try and remove the virus yourself with antimalware (technical users only), seek help from an IT professional, or even accept the damage and change passwords to secure information to prevent further security compromise.

“SIM swapping scam”

SIM card scams are more directed attacks that can be lengthy but very rewarding for the fraudster. Firstly, the fraudsters will try to gain valuable information about you through phising emails or gathering your metadata from social media, etc. After they have gained enough info, they will contact your cellular provider and request a new SIM card posing as you. Once they have this new SIM card they can gain access to anything you may have linked to your phone: banking, emails, phone calls, text messages, and even pictures. Setting up a PIN or password with your provider before any account management options can be accessed is the simplest way to prevent this, although using dynamic passwords can be very useful. If you have become a victim of a SIM card scam, contact your cellular network provider immediately and change all your passwords to any account linked to your phone.

“The Romance Scam”

The romance scam is a very personal attack that usually takes a long time to be successful, but the payouts can be large. With new social media outlets, meeting people online has never been easier and these fraudsters take advantage of that. They will slowly form a relationship with you purely virtually over the course of months, but eventually they will ask you for money in some way. This could be that they need to visit you but can’t afford the costs of travel, or a relative has become sick, or even some different variation with the same goal; getting your money voluntarily. Following a few rules to conversing over the internet with strangers can help you avoid this scam in the long run. Firstly, be wary of anyone that professes their love for you very quickly as to build a strong relationship fast. Also, as a rule of thumb do not send people money you have never met in person before. Another common tactic is to send you money by cheque, then ask for a portion of it back because the amount was larger than they anticipated. They will then cancel the cheque and you will be out all the money you sent back. It is nearly impossible to recover funds from this type of scam since it was voluntarily sent from you to the individual, so prevention is key.

“How to spot a phishing scam”

Phishing scams are designed to get information out of you that you wouldn’t otherwise make public. Convincing looking emails from fake companies or surveys can pry small tidbits of data from you that, over time, can seriously compromise your online profile.The best way to avoid these scams is by learning a few key red flags to look out for. Firstly, any demanding or threatening email asking for information from you is clearly not legitimate, as a company you trust would never be threatening if they needed you to update information. Warnings of account closure and other type of account warnings are also a usual red flag for phishing scams (if you are worried they are real, go to the account specified specifically). Alos, any suspicious senders/links/attachments are much better off to be ignored than trusted since any kind of data could be embedded within. If you have become a victim of a phishing scam, depending on the severity, anything from a simple password change or extreme measures like account closures may be required. Solving the issue is a broad since phishing scams can be directed at any part of your life, but being knowledgeable in prevention is always the best way to prevent further breaches.