RISK LESSON

Nancy Stevens – First Flight High School, Kill Devil Hills, NC

This material is based upon work supported by
the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

RISK

RISK SCENARIOS ACTIVITY

In this exercise, read each of the four Risk Scenarios provided. For each scenario, decide if 1) it has a low/medium/or high possibility of happening (use the provided chart), and 2) assess whether the resulting peril or injury would be low/medium/or high (use the provided table). Write the scenario number in the corresponding cell.

SCENARIO 1: MALWARE

It is a cool, crisp, Friday night in October. You tell your parents that you are picking up your friends and going to the Homecoming football game. You grab your jacket and, of course, your phone. Once you started driving, your parents insisted that the Life360 app is installed on your cell phone. Your parents justified the app as a safety measure, as it includes emergency roadside assistance, but they also made it a condition of access to the car and your cell phone. You have begrudgingly agreed to your parents' requirements because you want the freedom that driving offers you. Your mother's use of the app is pretty obvious as she emails the driving report to you whenever she sees that you have been speeding or used hard braking. She has even sent you text messages asking if you have been using your phone while driving.

After the football game, your friends want to go to a party. Since you did not discuss this with your parents, you explain your concern about the tracking app on your phone. Your friend, Katy, tells you that she has the same app and she simply uses a VPN to change her location. She shows you how to download and install free VPN software on your phone so that you can hide your actual location. While the VPN software installs, you don't notice that your web browser launches and closes. You return home later that evening and your parents simply ask who won the game.

In the following days, you notice that your Internet access seems to lag and pop-up ads start showing up in your web browser. Then you receive a "suspicious sign in prevented" email from Google. After a couple of weeks, you launch the web browser on your phone and there is no Internet access at all. Frustrated by the inability to use your phone, you take it to a computer repair shop. They remove a Trojan that was probably installed along with the free VPN software. They update

your Android system software, which was lacking recent security patches, and recommend that you purchase antivirus software. You were without your phone for three days and you paid a repair bill of $200.

SCENARIO 2 IDENTITY THEFT

You come home from school and find your mother on the phone and quite distraught. When your mother ends the call, she tells you that someone has stolen money from her bank account. The bank contacted her when it noticed unusual activity. Your mother immediately attempted to login to her account through the banking app on her phone and found that her password does not work. After contacting the bank, she found out that someone logged into her account, changed the password, and then started transferring funds.

Your mother tells you that she does not understand how this could happen as she had a long, complex password. The bank tells her that they are cancelling her credit and debit card. They advise her to change all of her passwords and check all of her accounts. She has spent the entire day on the phone. Your mother is upset and wants answers as to how identity theft happens. You ask your mother if she had noticed anything unusual on her phone. You ask her what devices she has used recently to login to her bank account. Your mother says once again that she can't believe that her account was hacked. As you talk with your mother, you ask if she has created new, unique passwords for each of her accounts. It is at this moment that your mother realizes that she had reused a password. Just a few months earlier, your mother's personal data had been exposed in the Marriott data breach. She had used the same password for her Marriott and her bank account.

Your mother spent over 20 total hours on the phone, changing passwords, cancelling credit cards, and closing bank accounts. A wire transfer of $10,000 has not yet been recovered. She filed a police report to protect herself from fraudulent debt that could appear on her accounts. She also filed an identity theft complaint with the Federal Trade Commission. The police recommended that she place a fraud alert on her credit report, keep close watch on her accounts, check the app permissions on her phone, and purchase identity theft protection. You suggest that your mother implement multifactor authentication on her accounts and consider purchasing a password manager.

SCENARIO 3 RANSOMWARE

It was Friday night in Mobile Alabama, and the air was thick and hot. The moon was full and the staff at National Hospital were preparing for a busy night. Amy was working the emergency room check in desk and trying to admit a patient

when her computer locked up. She turned it off and back on again, thinking that would fix the problem. It didn't. Another patient walked in, this time bleeding fairly profusely from his skull. She called Brad in the IT Department, who said that the entire network seemed to be locked up. By the time that Brad called back, Amy had two more patients needing to be checked in. Amy was starting to panic. Unsure what to do, she called her shift supervisor. The issue was so severe that the emergency room patients had to be diverted to other hospitals, potentially causing life-threatening delays and complications.

Officials at National Hospital reported that its network of three hospitals had been hit with a Ransomware Attack. Ransomware is a form of malicious software that infects a computer intentionally, thereby holding it hostage. The attack crippled the hospital's computer system. The hospital paid the ransom in bitcoin, approximately $65,000, in order to get the decryption key. They released a statement that teams have restored essential electronic systems related to patient care. The hospital began accepting patients on Thursday. Some of the nonessential systems such as email have not yet been restored.

Following an internal investigation of the incident, the hospital determined that an employee had clicked on a malicious link in a phishing email. The employee compromised his authentication credentials by clicking on the link. The attacker gained access to the network and deleted the backup files before encrypting the file system. The report recommended redundancy measures, increased reviews of system logs, password management policies, employee training, and a risk assessment audit.

SCENARIO 4 BUSINESS EMAIL COMPROMISE

Your father works for a regional construction and real estate firm. The company has less than one hundred employees. They have several residential developments in progress, along with land and home sales. The company has recently been the victim of a Business Email Compromise attack. BEC is a spearphishing attack that targets companies who conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives or high-level employees related to finance or involved with wire transfer payments are either spoofed or compromised through keyloggers or phishing attacks to do fraudulent transfers, resulting in hundreds of thousands of dollars in losses. These attacks use social engineering techniques to trick users. Real estate transactions provide opportunities for this type of attack due to the number of parties involved, reliance on email communication, and parties that may never meet in person.

One of the real estate brokers recently contacted his client's attorney to finalize the wiring of a down payment. The attorney contacted his client and found that the down payment had already been transferred. The broker immediately asked to see the wiring instructions. The email revealed that the client had been defrauded of their down payment and the real estate company was losing a sale.

 This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

NAME:_____

CYBERSECURITY RISK ASSESMENT CHARTS

POSSIBILITY OF PERIL

PERIL/ INJURY

		LOW	MEDIUM	HIGH
POSSIBILITY	LOW			
	MEDIUM			
	HIGH			

REASONING CHART

Scenario	Reason for Possibility Rating	Reason for Injury Rating
1 Malware		
2 Identity Theft		
3 Ransomware		
4 Business Email Compromise		