SPEECH OUTLINE FORMAT

Name: Brandon Burke

You Are Not Secure

Specific Purpose: The audience will be informed on security risks and implement mitigation strategies.

Introduction:

I. Warfare harms and destroys the lives of thousands of people. Warfare can be physical or digital.
II. This brings in the question of one's security. You may ask yourself, "Am I secure?"
III. Security is fundamental to protect the lives and property of people, yourself, and family.
IV. However, hackers and criminals have evolved their crafts to adapt to different security practices. This allows them to take control of many people's lives.

Thesis Statement/Central Idea: You are not secure. Your digital and physical security can be compromised, however there are mitigations that you can put in place to protect yourself.

Body:

(Connective: As we move into an online world, digital security has been on the rise.)

I. Digital Security

A. Wi-Fi is not secure.

1. An Israeli researcher compromised over 3,500 Wi-Fi networks. From a sample size of 5,000, over 70% were hacked with computers the researcher owned.

2. Let's apply this data to Norfolk, Virginia. The current population of Norfolk is 237,000 and the average household size in the US is 2.51 (United States Census Bureau, 2021). That means there are roughly 94,400 homes or apartments. If every home has a Wi-Fi connection, 66,100 Wi-Fi networks are vulnerable.

3. Once on a network, attackers have access to all your devices and personal information. They can grab your bank information, device passwords, and stalk you or your children just to name a few. *Show video of David Bombal hacking Wi-Fi with Android Phone.*

B. Accounts are not secure.

1. Attackers use a variety of techniques such as Phishing. According to various researchers "phishing is described as the art of echoing a website of a creditable firm intending to

grab user's private information such as usernames, passwords and social security number" (Mohammad et al., 2014).

2. These techniques often lead to data breaches. A data breach is an " incident involving unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data" (Sen & Borle, 2015).

3. Passwords are often reused from on different accounts a person owns. This could be Snapchat, Twitter, or Facebook. A successful phishing or MITM attack will compromise all accounts that you own.

(Connective: Digital security is not the only system that is flawed. Physical security is also a factor.)

II. Physical Security

A. Home security systems are not secure.

1. As we move into the digital age, more items are being connected to the internet. Home alarm systems are a part of this movement.

2. ADT, a home security company, offers devices such as cameras that can be accessed remotely. Cameras, an internet connected device, can be hacked by attackers. This could be used for stalking or information gathering.

B. Your physical computer is not secure.

1. Many people use laptops or desktop computers for school, work, or banking. However, these devices have open USB ports. That means any USB device can be plugged in the computer.

2. A Raspberry Pi Pico is a small computer that is the size of a thumbdrive. This tiny device can be plugged into the USB ports on your computer and can get full access to your system.

3. This allows the attacker to have access to sensitive information such as banking information and family photos. Uses HID and emulates a keyboard or mouse. Most famous BadUSB is Rubber Ducky. *Show video from NetworkChuck on the BadUSB.*

C. Social engineering makes you not secure.

1. "Social engineering is the art of exploiting the weakest link in information security systems (i.e., the people who use them)" (Bullée et al., 2018).

2. In simple terms, this means exploiting or taking advantage of a person.

3. For example, I can persuade a person that I am part of a banking company and try to steal their information. In this scenario, I am exploiting a person's trust. This could also be classified as Phishing.

(Connective: You might be scared that you are going to get hacked as I speak. The chances of getting hacked are very slim, but why take those risks? Let us implement mitigations.)

III. Mitigations

A. Use password complexity.

1. For Digital Security use, special characters, numbers, and letters for each password. Each password must also be different on Wi-Fi and digital accounts: banks, social media, etc.

2. For Digital Security use, password managers allow you to keep track of all passwords and can generate random passwords or all use cases. Password managers also flag a password if it is already used by another account you have and alert of password compromise.

B. Use two-factor / multi-factor authentication.

1. For Digital Security use, use your phone as an authentication source. The phone could receive text messages with a code that allows you to login in to your accounts on all platforms. A threat actor must have access to your phone in order to login to your account.

C. Use non-internet connected systems.

1. For Physical Security use, traditional methods of not using the internet for all appliances will eliminate the attack vectors. If a device is not connected to the internet, it is next to impossible for a remote attacker to gain access.

D. Use only trusted devices.

1. For Physical Security, only use trusted devices. Never plug in devices that are found on the ground, placed on your desk, or someone gave you. It is best to use your own devices for operations on your computer or work computer.

E. Be aware of what information you give

1. For Physical Security, be aware of what information is given to people. This prevents information from being leaked and compromised.

Conclusion:

I. Hackers and criminals evolved to counter security practices. This compromises your digital and physical security.
II. However, you can implement mitigations that can be put in place to combat these crimes.
III. Remember when I first opened this speech about warfare? It is only the beginning and it will continue in the near future. Take these practices and secure yourself and your family.

HONOR PLEDGE: I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violations of the Honor Code. I will report to a hearing if summoned. Signed: Brandon Burke

References

Bullée, J., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. Journal of Investigative Psychology and Offender Profiling, 15(1), 20-45.

Mohammad, R., Thabtah, F., & McCluskey, L. (2014). Intelligent rule-based phishing websites classification. IET Information Security, 8(3), 153-160.

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. Journal of Management Information Systems, 32(2), 314-341.

United States Census Bureau. (2021). U.S. Census Bureau Quickfacts: Norfolk City, Virginia. Census.gov. Retrieved November 2, 2022, from https://www.census.gov/quickfacts/norfolkcityvirginia