Hello everyone within the community, my name is Amy Holem and I am the new IT director for Pacts International. A brief little introduction about myself is that I am a video forensic analyst. I currently got my certificate back in February of 2020 and am capable of capturing the telecommunications of the criminals that are harassing, stalking and monitoring you. I also am able to prove the V2K, RNM, AI, and synthetic telepathy as well.

I currently have a patent in place that is creating a device to live stream these telecommunications. That means you will be able to press a button and hear the information that the criminals are passing between each other and also be able to gather names, departments, locations, vehicle descriptions, stalking techniques, how they are dressed and what they are currently doing, capture their weapon systems, and so much more. I have incorporated the link to the patent to receive your support. The faster that we create the patent, the faster you will be able to use the device. I would really appreciate the support, and I send receipts to everyone to show proof of payment, and so that you can use it on your tax returns as a donation.

https://www.gofundme.com/f/patent-live-stream-criminals-hackers-stalkers.

I also have been on numerous podcasts with many different groups and organizations and been helping people throughout the community for 3 years since 2017. I included one of the talk shows that you can review.

https://youtu.be/xhIG4iCHrQY.

I really want to get on a good start working with Pacts International, making sure that everyone is given proper techniques, knowledge, in law, evidence collection, and helping prove the torture programs that we all are forced to endure. Throughout the community false information is being spread and understanding the real terminology, real equipment, and how to report these crimes properly will help everyone get the proper investigations and legal help.

The first topic matter that I want to discuss with everyone is protecting your electronic devices., making sure that you all have the proper security measures into place to stop the hacking that is occurring. With all the people I have helped, over the years from different countries such as: Canada, Egypt, Argentina, Iran, Iraq, Vietnam, China, Russia, Poland, London, England, and the United states, everyone talks about their systems being hacked and compromised. So, I want to teach you how to avoid these topic matters.

Let's start off with the basic's first. Everyone knows the basics, or least have knowledge of the basics. First you want to make sure that you apply strong passwords onto your system. Make sure that you are using a two-way authenticator, when applying your passwords. It is also good to make sure that you also download software such as Malwarebytes which is a free source, firewalls, VPN, and encryptions onto your computer or mobile system. I will talk about IP's and changing IP's in a different discussion, that is a separate topic matter all on its own. I want everyone to remember that there are free sources that you can download onto your system. The most secure way is to buy the software and install it onto your electronic devices. That is the start and the basics that everyone should be doing to stop the criminals, hackers, agents, from attacking your device. If you cannot afford the software you can always go to SourceForge.net https://sourceforge.net/. and they will give you suggestions for the software application that you are looking for.

Here is a list of anti-malware products.

- **BitDefender—*www.bitdefender.com*.**
- **Kaspersky Anti-Virus—*www.kaspersky.com*.**
- **Webroot Antivirus—*www.webroot.com*.**
- **Norton AntiVirus—*www.symantec.com/norton/antivirus*.**
- **ESET Nod32 Antivirus—*www.eset.com*.**
- **AVG Antivirus—*www.avg.com*.**
- **G DATA Antivirus—*www.gdatasoftware.com*.**
- **Avira Antivirus—*www.avira.com*.**
- **McAfee Endpoint Protection—*www.mcafee.com*.**
- **Trend Micro—*www.trendmicro.com*.**
- **Microsoft Security Essentials—*www.microsoft.com/security_essentials*.**

firewall solutions available.

- **Palo Alto Networks—*www.paloaltonetworks.com*.**
- **Cisco Systems—*www.cisco.com*.**
- **SonicWALL—*www.sonicwall.com*.**
- **WatchGuard Technologies—*www.watchguard.com*.**
- **Check Point—*www.checkpoint.com*.**
- **ZyXEL—*www.zyxel.com*.**
- **Netgear—*www.netgear.com*.**
- **Juniper Networks—*www.juniper.net*.**
- **DLink—*www.dlink.com*.**
- **MultiTech Systems—*www.multitech.com*.**

Make sure you check the most recent updates and do research before downloading. Some companies have been breached recently just in 2020, so make sure that you do any research if you are not familiar with the products and download the right one that suits your needs.

Now that the basics are out of the way lets discuss other areas, such as different types of attacks, techniques, and ways to solve the issue.

- Cyber criminals and cyber attackers use a number of different tools to exploit, discover weaknesses throughout your electronic devices. Electronic devices are anything from a computer, iPad, tablets, phones, laptops, or anything that has Bluetooth connections. Anything with Bluetooth is hackable, so when you are not using a Bluetooth device make sure that you turn it off in your settings. It is also wise to turn off the remote access onto your systems. This can be found and located in your control panel of your computer systems. You can type remote access into the search bar in the control panel and turn off the settings. This removes a backdoor access into your system. Back to the electronic devices and hardware that cyber criminals and cyber attackers use. They use devices such as:

- Protocol analyzers
- Port scanners
- OS fingerprint scanners
- Vulnerability scanners

- Exploit software
- Wardialers
- Password crackers
- Keystroke loggers

One of the best books that you can use on this topic is **Fundamentals of Information Systems and Securities.**

Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (3rd ed.). Burlington, MD: Jones and Bartlett learning. Retrieved from https://aiu.vitalsource.com/#/books/9781284128567/cfi/6/24!/4/2/6/16/14@0:69.3.

There are also a number of different activities that can cause the security breaches within your system. Some of these security breaches are known as:

- Denial of service (DoS) attacks
- Distributed denial of service (DDoS) attacks
- Unacceptable web-browsing behavior
- Wiretapping
- Use of a backdoor to access resources
- Accidental data modifications

Two methods of active wiretapping are as follows:

- **Between-the-lines wiretapping**—This type of wiretapping does not alter the messages sent by the legitimate user but inserts additional messages into the communication line when the legitimate user pauses.
- **Piggyback-entry wiretapping**—This type of wiretapping intercepts and modifies the original message by breaking the communications line and routing the message to another computer that acts as a host.

Now let's talk about cookies onto your system, not all cookies are bad no matter what you think, some are necessary to transfer files back in forth from your folders setting. A **cookie** is simply a text file that contains details gleaned from past visits to a website. Cookies have value, since HTTP is a stateless protocol (one that can't retain data from one visit to the next), so a data file cookie is used to keep a small record of the last visit. Cookies do not directly perform malicious acts. Cookies cannot spread viruses, nor can they access additional information on the user's hard drive. The thing to remember about cookies is that the more you surf the web the more they are collected. So, it is wise to remove these cookies to keep your information secure. One way to make sure that your computer is secure is always use a website with the **HTTPS://** If you use a webpage that is **HTTP://** chances are it is not a secure site and may have hidden vulnerabilities within the page. Another thing you can do to secure your system, is go to the hamburger bar on the internet or the three dots, go to history, and clear browsing history. You can also change this in your settings in the control panel to have them deleted every hour, 5 hours, day, week, month, etc.…

Another thing you can do to protect your system is back in the hamburger on the right-hand side of the internet. You can go to your extensions and delete any unknown extensions that are on your system.

Here is a list of the domain and the threats that are applicable to the domain.

Common threats and vulnerabilities in the seven domains of an IT infrastructure.

DOMAIN	COMMON THREATS AND VULNERABILITIES
User domain	Lack of awareness or concern for security Accidental acceptable use policy violation Intentional malicious activity Social engineering
Workstation domain	Unauthorized user access Malicious software introduced Weaknesses in installed software
LAN domain	Unauthorized network access Transmitting private data unencrypted Spreading malicious software
LAN-to-WAN domain	Exposure and unauthorized access to internal resources from the outside Introduction of malicious software Loss of productivity due to lack of Internet access
WAN domain	Transmitting private data unencrypted Malicious attacks from anonymous sources Denial of service attacks Weaknesses in software
Remote Access domain	Brute-force password attacks on access and private data Unauthorized remote access to resources Data leakage from remote access or lost storage devices
System/Application domain	Unauthorized physical or logical access to resources Weaknesses in server operating system or application software Data loss from errors, failures, or disasters

Malware comes in many different forms and new tactics and methods are coming out everyday to attack someone's system. There is great anti-malware systems that one can use against these attacks. Some websites that you can go to learn more about these types of attacks, and how to safeguard your system is:

- **National Cyber Security Alliance (NCSA)**—***www.staysafeonline.org***.

- **United States Computer Emergency Readiness Team (US-CERT)—*http://us-cert.gov*.**

Here is a list of anti-malware products.

- **BitDefender—*www.bitdefender.com*.**
- **Kaspersky Anti-Virus—*www.kaspersky.com*.**
- **Webroot Antivirus—*www.webroot.com*.**
- **Norton AntiVirus—*www.symantec.com/norton/antivirus*.**
- **ESET Nod32 Antivirus—*www.eset.com*.**
- **AVG Antivirus—*www.avg.com*.**
- **G DATA Antivirus—*www.gdatasoftware.com*.**
- **Avira Antivirus—*www.avira.com*.**
- **McAfee Endpoint Protection—*www.mcafee.com*.**
- **Trend Micro—*www.trendmicro.com*.**
- **Microsoft Security Essentials—*www.microsoft.com/security_essentials*.**

There are also many different types of malware that exists, some of the different malware are: viruses, worms, trojan horses, rootkits, and spyware. I will provide a link to websites that you can visit to help you protect your system to those that cover all these topics.

The first form of attacks that is the most used by hackers is using viruses to gain access through the network. These attacks do not only happen to people who owns businesses but personal computers as well. Hackers have the motivation, knowledge, to send the viruses to either personally attack people for revenge, vendettas, beliefs, and a way to maintain leverage against the person or company. A virus is a "software program that attaches itself to or copies itself into another program."(Kim, D., &Solomon, M. G., 2018). There are many different ways that one can protect your system from viruses the most common ways are, using a VPN (virtual private network), firewall, and malware apps. There are additional measures as changing and applying pop-up blockers on your system. One should always clear your cache and browsing history from the internet as well. One can apply it into their internet settings in the control panel. When applying this to a network, one has to go through the correct applications in the settings in the control panel of the computer that a person is using. Another way to implement the security measures is buying the software and services and install them into your computer. There are free applications that one can download, one has to make sure they are valid and do not contain hidden viruses as well. (Microsoft Corporation, 2020). https://support.microsoft.com/en-us/help/17228/windows-protect-my-pc-from-viruses. Some of the best tutorials are from Microsoft, with videos included, make sure that you visit their site and learn many techniques to protect your system, including router settings. Which I will discuss at a later time, once again it is a topic matter that deserves it's own report.

The next form of attacks is known as a worm, a worm is a "self-contained program that replicates and sends copies of itself to other computers, generally across a network, without any user input or action. ."(Kim, D., &Solomon, M. G., 2018). Some ways to protect yourself is to keep all your software, applications, your settings are up to date. Updating the system allows overwrites of current codes that will delete any worms that are attached.

Some other avenues are removing extensions in your browser of the internet and add-ons as well. Also check your firewalls and make sure they are updated too. You also can create a guest access in your router and DNS settings. To install this into your settings into your router, one can access and change the SSID connection and hide your network from plain site. Creating a separate network using different IP addresses will allow additional safety measures to protect your computer. For the extensions on your browser, go into the hamburger menu and go through the extensions and delete anything that you do not recognize on your system. (GELINAS, J., 2020).

Buffer overflows are "vulnerabilities that deal with buffers or memory allocations in languages that offer direct, low-level access to read and write memory." (Benjamin, K., 2017). Unfortunately, we cannot use the same techniques to find and detect the buffer overflows, these are written codes using C and machine assembly writing. One has to have the knowledge of writing code to remove and delete the overflows from your computer. Some ways to protect yourself is to use different codes such as Java, Python, and .NET. If you are a person that is experienced writing code in the different languages, then you will be able to find and detect the buffer overflows and remove them from your system. (Benjamin, K., 2017). https://dzone.com/articles/how-to-detect-prevent-and-mitigate-buffer-overflow. If you are interested in learning how to read and write the code this is a great first step learning tool. https://www.w3schools.com/. This will help you learn the basics for any code writing.

Another type of known attacks is known as networking traffic pilfering. This is a way to steal information using a thumb drive or flash drives. Downloading information from an unattended computer is the easiest way to access and steal the information the criminal wants. The easiest way to protect yourself from this kind of an attack, is to secure your system with the proper security measures as firewalls, VPN, and malware. Encryptions are key, to protection. Make sure that all information on your computer is encrypted and cannot be bypassed. Another way is to make sure in the policies and procedures of a company, that you turn off your device before walking away so no one has easy access. (Tan, L., 2007). https://www.komando.com/privacy/ways-to-keep-hackers-off-of-your-network/738560/.

This brings me to the last type of attack which is a man-in-the middle attack. This type of an attack occurs to often and is easily implemented. This is where there is middleman between two conversations pretending to be the other person. The two other people have no concept that they are talking to the criminal, instead of each other. This is mainly done by impersonating internet access, a person logs into an open source and the hacker can grab all information they need. In order to prevent this from happening one should always make sure that they are always using a HTTPS inside their browser for searching. If it is an HTTP the site might not be secure and is easier hackable. (Publico, R., 2017).

Truth is there is more than one way to stopping these criminals, making sure that you take that proper steps to add extra security as Malwarebytes, encryptions, strong passwords, VPN, firewalls, and even set up your router correctly, is just the beginning process to protecting your computer or networking system. Implementing the other suggestions can make sure that your network and system are working correctly and in a

safe manner as well. So, make sure that you follow the suggestions and give those hackers a run for their money.

I like to thank you for your time and look forward to our next discussion.

References:

Benjamin Kerestan, B. (2017, July). How to Detect, Prevent, and Mitigate Buffer Overflow Attacks. In *DZone*. Retrieved from https://dzone.com/articles/how-to-detect-prevent-and-mitigate-buffer-overflow.

GELINAS, J. (2020, May 16). 6 ways to keep hackers off of your network and computer. Retrieved from https://www.komando.com/privacy/ways-to-keep-hackers-off-of-your-network/738560/.

Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (3rdrd ed.). Burlington, MD: Jones and Bartlett learning. Retrieved from https://www.amazon.com/Fundamentals-Information-Systems-Security-Assurance/dp/0763790257.

Microsoft Corporation. (2020). Help prevent viruses from getting on your PC. In *Protect my PC from viruses*. Retrieved from https://support.microsoft.com/en-us/help/17228/windows-protect-my-pc-from-viruses.

Publico, R. (2017, March 1). What is a Man-in-the-Middle Attack and How Can You Prevent It?. Retrieved from https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack.

Tan, L. (2007, June 22). Tips to prevent data pilfering. In *ZDNet*. Retrieved from https://www.zdnet.com/article/tips-to-prevent-data-pilfering/.