**Personal Cybersecurity Threats and its Management**

**Thesis Statement:**

As we evolve to the digital 21st century there are many personal cybersecurity threats that we can think of and it’s growing at very fast. How safe is our devices are and how can we make them more safe for us. A good cybersecurity architecture alone is not going to stop cyberattackers who are targeting an enterprise, our home and other electronic devices. The attempting to defeat its cyberdefenses. Cyberdefense capabilities need to be applied in ways that disrupt, detect, delay, and defeat targeted cyberattacks. It takes 20 years or more to build a reputation and few minutes of personal cybersecurity-incident to ruin it.

Today, the term is almost exclusively used to describe information security matters. Because it’s hard to visualize how digital signals traveling across a wire can represent an attack, we’ve taken to visualizing the digital phenomenon as a physical one. A cyber-attack is an attack that is mounted against us (meaning our digital devices) by means of cyberspace. Cyberspace, a virtual space that doesn’t exist, has become the metaphor to help us understand digital weaponry that intends to harm us. What is real, however, is the intent of the attacker as well as the potential impact. While many cyber-attacks are merely nuisances, some are quite serious, even potentially threatening human lives.

1. **PHONES**

At this time mobile phones are treated as the essential thing of our lifestyle like we eat or sleep we need phones too right. Smartphones or mobile phones with advanced capabilities like those of personal computers (PCs) and are appearing in more people’s pockets, purses, and briefcases. One example is this year’s Valentine’s Day attack, in which attackers distributed a mobile picture-sharing application that secretly sent premium-rate text messages from the user’s mobile phone. One study found that from 2009 to 2010, the number of new vulnerabilities in mobile operating systems jumped 42 percent. The number of attacks on mobile phones is increasing, and countermeasures are slow to catch up.

1. **Malicious apps:**

When we visit Google play or app store to download apps that look harmless but these apps ask for permission generally require some kind of access to files, cameras, GPS or folders on the mobile devices. All of us will glance at the list of permissions and agree without reviewing them in detail. This lack of scrutiny makes our devices more vulnerable to mobile threats. Malicious apps from a campaign called “Agent Smit” have been downloaded to 25 million android devices according to new research by cyber security firm checkpoint. The malicious apps that were downloaded from the third-party source most of the games distributed by a Chinese group with a legitimate promotion of their apps outside the platform. About 300,000 devices were infected in the US alone from “Agent Smith”.

This malware copy all popular apps on the phone including WhatsApp and popular Web browser that users using injected its own malicious code and replace the original app with the weaponized version. These hijacked apps would still work just fine, which hid the malware from the users. Google already fixed at least one of the android exploits used by “Agent smith” nicknamed Janus in 2017 but the fix hasn’t made its way onto every android phone.

To remove these kinds of threats or malware happening to our phone user must update these phones, 87% of Android devices in 2015 were using out-of-date versions of the operating system which cause the Vulnerabilities in the phones. If you are downloading a third party app read its permission what the app wants to access on your phone if that does not look good “Do not install that third party app”.

## No password protection:

## This seems like an unusual threat to person who’s using phone right now, why I need protection from in my phone right but if your phone get lost unfortunately than the thieves will easily access all your data and information stored in phone. It might be shocking but only 34% of people don’t use a password to lock their phone. Data and the personal information is the most important thing your phone which any person can access it if there is no password on your phone. Password should be strong and hard to guess and it should have an alphabet, capital letter and some numbers too, which will make it harder to guess for anyone. Smartphone should force users to put password on their phone at least at the time of restart or shutdown. Passwords are like underwear make them personal, don’t let people see it, make them exotic, and change them on a regular basis.

## Public Wi-Fi

“Free Wi-Fi” is a word that we see everywhere we go to cafes, libraries, restaurants, and hotels. We maybe won’t see any welcome sign there but we will definitely see free Wi-Fi sign for sure these days. This threat occurs to phones, tablets, and laptops. It is like “stranger danger” we have to be always wary about which network we connecting to. There are basically two kinds of public Wi-Fi networks: secured and unsecured. An unsecured network can be connected to within range and without any type of security feature like a password or login. Conversely, a secured network requires a user to agree to legal terms, register an account, or type in a password before connecting to the network. It may also require a fee or store purchase to gain access to the password or network. Regardless of the connection type, you should [always use public Wi-Fi with caution](https://community.norton.com/en/blogs/norton-protection-blog/risks-public-wi-fi). Now days creating a fake free Wi-Fi is very easy, just have to download software for hotspot and pick a name for a network that looks entirely legit and it's done. Now what they do is to trick people of connecting to a network that looks authentic enough but is actually controlled by hackers like as site you can say Facebook, Twitter and many more. But these people are mostly after your money, so as you open any bank or payment site they will redirect you to their fake site as you fill all your credential details there mostly will be error or you will be redirected to another page. By doing this they have access to all your personal information either its credential or not. Sometimes they ask the user to make an account on their free Wi-Fi providing site by Google or Gmail logins so they can get your user name and password. Let’s see one image which shows this example

## Public Wifi

**How to be secure from public WIFI**

More than 70% of phone, tablet or laptop users were reported to connect to unsecured public networks in 2016. The things we can do to protect ourselves from these threats by never sharing bank or any credential details on public Wi-Fi even it says it highly secured. If we are using public Wi-Fi more often than we should download virtual private networks (VPNs) to encrypt data sent on untrusted networks and ensure mutual authentication of client and server. Everyone should change their password after connecting to a public network with the same username or password. If you don’t have access to a VPN, making sure you are only visiting encrypted sites can also help protect your data from some of the threats outlined above. Look for HTTPS at the beginning of a website’s address. This means the connection between the browser and the web server is encrypted, so any data that is submitted to the website will be safe from eavesdropping or tampering. Most browsers also include a padlock symbol at the beginning of the address to indicate the site uses encryption. When connecting to public Wi-Fi, there’s a setting on your device that enables sharing over the network. It’s unlikely that you want to share anything publicly, so you’ll want to disable this setting. If you’re on Windows, you can do this by choosing “Public” the first time you connect to the Wi-Fi. This will lock your connection to keep your computer from sharing sensitive data. On other devices, you can check your Control Panel to change the share settings. One of the basic rules of security is that if you don’t need something connected to a network, don’t connect it. When you’re finished working online, turn Wi-Fi off on your laptop, tablet, or smartphone. It’s a nice security habit to get used to when you’re using untrusted networks (if you have to use them at all), and it’ll also save your battery. It’s [easy to do in macOS](http://lifehacker.com/disconnect-from-a-wi-fi-network-in-os-x-without-turning-1714736241), and in Windows you can even set your laptop to [automatically turn Wi-Fi back on](http://lifehacker.com/windows-10-can-automatically-turn-wi-fi-back-on-after-a-1788015284) after a short time offline.

## Social Site

## Social media such as Facebook, Twitter and Instagram, has shown explosive growth in recent years. Twitter has 330 million active user and Facebook have more than 500 million user active till now. Social networking sites are now a primary source for communicating and keeping in touch with friends and family. When utilizing a social networking website, people have the option of sharing personal details with friends and followers. While sharing some information is okay, other facts can reveal too much about who a person is. For the sake of personal safety, one should never reveal their date and place of birth, home address or phone number, as this could put them at serious risk for identity theft and fraud. Social media has (rightly or wrongly) become an important part of our world, with a wide number of digital platforms encouraging us to broadcast all aspects of our lives. But are we sharing too much? Does posting a photo in front of the airport departure sign increases your risk of burglary while away on vacation? And what about reputation over the last few years we’ve seen countless stories in the media not only about celebrities but also ordinary individuals who’ve lost their jobs after posting something seemingly innocent on sites like Twitter. While there’s no clear cut answer, we think ‘less is more’ works well here don’t feel pressured to post more than you’re comfortable with, knowing that what goes on the internet can be almost impossible to delete later down the track. All these social sites are growing day by day and the threats are also increasing very rapidly. Let’s see some threats regarding social sites.

## Spreading scams, malware and hacks

Social sites are widely used these days so the cyber criminals targeting the social site handlers. They send you some URL or link of any possible thing you can imagine for example if you are a movie fan there will be a link of your movie. When you click on these links they take you to the malicious sites it can be either good or bad depending on the cyber criminals. Pop-ups occur when someone is browsing the social sites and sees a small graphic or ad appear on their screen. Usually, pop-ups are related to the content being viewed and link to another website with similar content or merchandise related to the content. Malicious pop-ups can be terribly intrusive, making it difficult for the user to close the pop-up window. These pop-ups may display a message stating that the computer is infected with malware and offer a phone number for help with removing the malware. Often, the cybercriminals make pop-ups look like they come from a trusted source, such as our own Norton products, in hopes of appearing to be legitimate. Every major news or TV shows have their account on these social sites which makes them more connected to the users. A recent social **media scam involved false reports that the actor Rowan Atkinson had died. (The Mr. Bean and Blackadder actor is still**[**very much alive**](https://www.snopes.com/fact-check/rowan-atkinson-death-hoax/)**.) It’s not just about some fake news, fake add or fake review it can be about anything. Recently a Filmmaker Tyler Perry recently posted a video to his Facebook account warning fans not to fall victim to giveaway scams using his name.** Now days, good source of news are these social networking sites and if you want celebrate any day like valentine day or any day that you like most the links of every kind possible will be there, what to do on a specific day, what to wear, what to shop for that for that day and so on, you can find all kinds of scams there for everything. Malware attacks and hacks are common for social sites these days many people accounts get hacked. The hacker do mostly two things these days either they take some personal data that is saved on that account or they post on behalf of you in these social sites looking like you did this.

**How to protect against malware attacks hacks and scams**

## Do not click any links or download any attachments in the suspicious email. Instead, open up your web browser and go to the website in question by typing it into the URL bar. Be vigilant and pay attention. Phishers have been known to use real company logos to make their communications seem legitimate. They also use spoofed email addresses, which are similar to the actual company’s address. However, the address may be misspelled slightly or come from a spoofed domain. Examine the message closely. Look for obvious signs of fraud such as poor spelling, unprofessional imagery, and bad grammar. Remember, when in doubt, never click on the pop-up. Instead, open up your antivirus software and run a system scan.  Protect your web browser with extensions, updates, advertisements, said [Menlo Security](https://www.menlosecurity.com/) CTO Kowsik Guruswamy, are one of the major malware risks to internet users. He says you should install an adblocker and use it on unfamiliar or questionable sites to ensure your holiday shopping is safe. He also recommends a transparency extension like [Lightbeam](https://www.mozilla.org/en-US/lightbeam/" \t "_blank), which keeps an eye on who (and what) is tracking you online. Also be sure to keep your web browser up to date. A security patch may be all that stands between you and disaster.

## Online shopping

## Everyone loves shopping and online line shopping is the most used now day. Online shopping increasing day by day till now there are 1.92 billion people who shop online. People say its 100% safe for online shopping but it’s likely not even 60-70% safe. Anything we do online now like providing details like email address, shipping address, phone number and credit card information, all of our information becomes prey for cyber criminals. Let’s talk about some most common security risks of online shopping.

## Fake online stores

## Cyber criminals are making fake shopping platforms to trick users into wasting money or revealing sensitive data. What they do is they try to looks like some legitimate retailers or claim they work with them or imitate our required online stores and sell products like them. There is two types of thinking or scam behind this attempt either they will take all the data you type in regarding credit card details and personal information. Some time they also ask for social security number. The other thing they do is show you your required product that is advertised which don’t actually exit. So, if you buy something you will never git it or will get something that you didn’t order for or if you are lucky enough you can get an empty box. There is no guarantee for above things may happen to you or maybe not it depends on the cybercriminal what he is looking for money or data information or maybe both.

## Always look for trusted retailers in online shopping. There will be like ten or more than that retailers that are selling the same items for very less amount but choosing the right and trusted retailers what we are looking for. If we do online shopping we should never save our password or credit card details on our computer or phones. Suppose our phone or laptop get lost the person who find this will have a free amazon account too with all the free stuff.

## Adware

## Adware can be defined as the pop-up ads that can be related or unrelated to our subjects. Malicious website contains pop-ups which either giving you free product that you are choosing in your cart or maybe a free trip for some days. In these pop-ups user are requested to share their personals details so you can continue to your required product. Some pop-ups contains malware file, if you clicked on pop-ups your devices get infected with spyware, ransomware and keyloggers.

## How to stay safe on online shopping

### [Trust your gut](http://us.norton.com/clubsymantec/library/article.jsp?aid=cs_shop_safely_online): Just like you wouldn't go into a store at the mall that you don't recognize and seems a little off to you, don't shop at stores online that give you a bad feeling and appear shady. If at any time during the shopping or checkout process you feel like the site is asking for too much personal information, just quit the transaction and leave the site. You may hate to leave behind a really good deal, but the money and time you could lose if someone gets your credit card information will definitely cancel out the benefits of a sale price. If the site looks like it was designed in the '90s, has a weird address, or fills your screen with pop-ups, just forget about it.

### [Use a virtual credit card number](http://lifehacker.com/5831160/use-virtual-credit-card-numbers-to-shop-safely-online-keeping-in-mind-the-downsides): If you just have to have something on a site you're unfamiliar with, there's a neat little thing called a virtual credit card number that allows you to shop online without exposing your real account number. Several banks offer these kind of temporary credit card numbers that allow you to set the amount and time frame for a purchase and then send you a card number to use online. You minimize the damage since the number will expire relatively quickly and has a lower maximum spending amount and your real credit card number is still secret. At the very least, limit your online spending to one traditional credit card so the damage and hassle is contained to one credit card Company if you do get hacked.

Use two-factor authentication: If an online store offers [two-factor authentication](https://www.tomsguide.com/us/how-to-enable-2fa,news-26607.html), use it. (Amazon now does.) Yes, it may mean going through an extra step, such as typing in a code texted to your phone or generated by [an authenticator app](https://www.tomsguide.com/us/google-authenticator-how-to-use,news-26819.html), but it adds a layer of security. It'll make it much harder for anyone who has your password to access that account. [Change your passwords regularly](http://www.wisegeek.com/how-often-should-i-change-my-password.htm)

## GPS

Global Positioning System or GPS is important part of our life now. If we want to go to a new place or any address, restaurants, gas station or any possible place we can think of GPS will get us there. We use GPS in mostly two things cars and phones. These two devices are equipped with a GPS systems and becoming increasingly vulnerable to accidental interference or deliberate jamming, raising concerns about reliability and security. However low powered GPS signals are easily drowned out by other sources which are increasing in number. GPS signals are weak and can easily be outpunched by poorly controlled signals from television towers, devices such as laptops and MP3 players, or even mobile satellite services. One of the most common human errors when it comes to using a GPS device is overconfidence in how smart that navigation system is or isn't. Why plan when your GPS will tell you where to go? Well, GPS devices are fallible; they're made so by satellite communication errors and outdated or inaccurate maps. Even when maps are current, some mapping and navigation information doesn't take into account road types. With this type of software error, the road that may look like the shortest distance between Point A and Point B might actually be an unpaved private drive. If your GPS device doesn't recognize it as such, it could add the road to your route. Because of these factors, drivers find themselves driving on unsafe terrain and into other hazards, such as artificial lakes or train tracks. The more confident you are in what your GPS device tells you, the less likely you are to notice something's wrong. Accident risk increases when drivers take their GPS device's instructions too literally: Warnings of "when possible, make a legal U-turn" send some veering into oncoming traffic.

## Typical GNSS Vulnerabilities

## Cars

## Cars now days run on data as much as they depend on oil or gasoline. It would be easy to say that a modern car is a computer on wheels, but it’s more like 30 or more computers on wheels. The most basic cars today have at least 30 electronic control units and luxury cars have more than 100. These electronic controls the engine, transmission, brakes, transmission, safety system such as airbags, diagnostics, navigation, climate, and sometimes communication and entertainment system. Of course, the nightmare scenario is that a hacker can take control of someone’s vehicle and cause it to crash. In July 2015, wired magazine broke the story that hackers had taken control and killed the accelerator of a Jeep in motion on the freeway but more of these things happen in an episode of Homeland than our daily lives. The most common near term consequence of vehicle hacking could be auto theft. Hackers already created an OnStar communication system that allows a hacker to track, unlock, and start the vehicle. All he had to do is place that device in an inconspicuous place of the target vehicle. This used to track a driver’s personal habits and schedule. This information could be used to plan burglary when a driver is away from home and used for extortion.

## ****Phones****

**Phones are devices that use GPS all the time. The threats are as same as tracking your schedule, what place you visited and which places you marked as a home, office or safe. In some cases they exposing location information, device model and type information, IMEI numbers, phone numbers, custom assigned names, audio recording, and images of the user. When it comes to images and audio recordings, the exposures happened via open directories on the affected service’s website. The problems were compounded by the fact that most of the vulnerable services had no contact information, likely because they are re-sellers. At first, only one intermediate vendor – One2Track – responded and promptly fixed the problem over the weekend. ThinkRace, one of the largest vendors for these GPS tracking devices, eventually agreed to fix four domains just hours before the public disclosure was to take place. This delayed disclosure by 24-hours. The researchers believe that ThinkRace is the original developer of the location tracking online service and software, licensing it out to others. However, they don't have any control over the vulnerable websites that were discovered, other than the four they promised to fix.**

**As long as the online service managing your device is still vulnerable changing your password will not matter and there is unfortunately not much you can currently do to protect yourself besides stopping to use the device.**

1. **Data threats**

**Data is the most important thing for us nowadays and cybercriminals are attacking these data either it is stored on computers, phones, tablets or laptops. The data we have is worth those devices or maybe more for us. There are many different threats to our devices and data stored on them as we connect them to the Internet. Unless our devices or computer system are highly protected, they all are vulnerable to threats like some can copy, delete or edit your files without your permission. As our data increase day by day the threats to it also growing very fast.**

Backing up your data regularly is an overlooked step in personal online security. The top IT and security managers follow a simple rule called the 3-2-1 backup rule. Essentially, you will keep **three** copies of your data on **two** different types of media (local and external hard drive) and **one** copy in an off-site location (cloud storage). If you become a victim of ransomware or malware, the only way to restore your data is to erase your systems and restore with a recently performed backup. **Some of the data threats are**

1. **Virus and Malware**

## Every present devices have occurred above threats. Viruses and malware are a piece of software that is designed to stop or disrupt the normal working of a computer or device. Virus is like a biological virus they are passed on from one infected machine to another. Viruses can hit us from online downloading from the internet, attaching USB memory sticks or emails. Viruses can also replicate themselves. A computer virus is more dangerous than a computer worm because it can make changes or delete your files while worms only replicate itself without making changes to your data or file. Example of virus areW32.sfc!mod, ABAP.Rivpas.A, Accept.3773 and many more. The working of malware is designed to cause damage to a computer or a connected network pc or any other devices. Whenever a malware term is used means a program is designed to damage your computer or any connected device to the internet.

## virus Whenever downloading a file from any device make sure the files are provided by the good vendor and you should have an updated antivirus installed. Misleading applications misguide you about the security status of your computer and show you that your computer is infected by some malware and you have to download the tool to remove the threat. As you download the tool it shows some threats on your computer and to remove it you have to buy the product for which it asks some personal information like credit card information etc. which is dangerous. Always made data backups or files or anything that is stored on that device that will make you recover your data if something malicious happened.

## ****Phishing****

**Phishing is a type of email fraud method which is used by criminals to send out some legitimate-looking emails regarding your concern. They will use that email in an attempt to gather personal information and finical information from you. The emails come from a trustworthy web site that is spoofed by phishers including PayPal, eBay, Msn, and Yahoo. As its name suggests it will lure you into the emails which they have sent appearing to be a well-trusted web site, as you clicked on these links you will be redirected to the shopping websites where you have to provide passwords and credit card details. Some of us believe it’s a trusted website that gives them bait what they are looking for.  
There are many steps can be taken to avoid Phishing.   
Always be careful about opening emails from unknown sources. If someone sends you a cheap eBay or Amazon product check there official site and confirm them by calling on their helplines. When shopping on the Internet make sure that you use sites where the data is encrypted when you send personal or financial details. You can tell this from the lock that appears at the bottom of the browser window. Always make sure that antivirus and other protection software is up to date and turned on.**

## BYOD (Bring Your Own Device)

Let’s imagine, you have just back to work from being on annual leave and you want to show your holiday photos off to your colleagues. You could just plug in your USB Flash Drive and begin your presentation but why is this usually considered to be a bad idea? USBs are the devil. They just are.

It’s simple, you have no way of knowing what could be lurking on that pen drive and it could be harmful. Your home computers security software may have not detected a virus like Malware, it has now infected your storage device and will continue to propagate across any enterprise network that you connect it to. A study conducted by HP identified that 97% of employee’s devices contained privacy issues and 75% did not have sufficient data encryption. This doesn't just refer to storage devices; laptops, mobile phones, tablets and even wearable technology all have the capacity to become hazards. Many organisations have created BYOD policies as there can be benefits such as using personally owned, company enabled devices can reduce expenditure from issuing employees with solely company owned devices. The risks present themselves when a personally owned device is used for both work and non-work purposes simultaneously - in short, if the device is compromised by a third party then your software could easily become compromised too allowing the perpetrators to access sensitive documents and files. The most common way of reducing these risks is to ensure any BYOD policies also contain addition security measures to be installed on any devices. This does allow protection for the personal usage of the device but most importantly increases the security of company operated applications and software.

**Why Personal Security Fails Against Advanced Attacks**

Modern operating systems are too large and complex to be fully protected. Security statistically reduces the percentage of compromised endpoints, but cannot eliminate them altogether. Endpoints are always susceptible to being compromised. For every defensive capability, there is a corresponding attacker tool, technique, or procedure. There is no *perfect* or *unbreakable* defence. Real-world attacks often use relatively simple attack methods. Viruses, Spear phishing, Published vulnerabilities, Credential theft, Web site compromise. Even with data encryption, high-assurance hardware, and physical isolation, enterprises remain open to more basic formats of attack.

The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: “Personal Cybersecurity is much more than an IT topic.” Technology trust is a good thing, but control is a better one. So let’s control the technology that is around us.

## References:

## <https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>

## <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/>

## <https://us.norton.com/internetsecurity-online-scams-how-to-protect-against-phishing-scams.html>

## Corvallis Microtechnology, Inc. 2000 "Introduction to the Global Positioning System for GIS and TRAVERSE." <http://www.cmtinc.com/gpsbook/index.htm>

## <https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/>

## Carey, Tanith. 2008. "SatNav danger revealed: Navigation device blamed for causing 300,000 crashes." The Mirror. [http://www.mirror.co.uk/news/top-stories/2008/07/21/satnav-danger-revealed-navigation-device- blamed-for-causing-300-000-crashes-89520-20656554/](http://www.mirror.co.uk/news/top-stories/2008/07/21/satnav-danger-revealed-navigation-device-%20blamed-for-causing-300-000-crashes-89520-20656554/)

## Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam (2018)- Enterprise Cybersecurity Study Guide-Apress

## Kim J. Andreasson (2011) – Cybersecurity Public Sector Threats and Responses-CRC Press