Mayur Suresh

Professor Ola Ajaj

CSC-301-02

11/29/2021

Privacy Issues in Cyberspace

Over the years of using the Internet and technology, I have seen many times I have seen privacy issue on the internet as are most of the population that use the internet. I personally have seen many types of privacy related issues such as phishing, workplace monitoring and organizations collecting information about web browsing behaviors.

During the summer break of 2020, I got a phishing email. This email was from a user who had distinct a email-id made of up of numbers and letters in no necessary order. This email started with saying that they had installed a trojan software installed on my computer gathering all pornographic data from my history and they were going to send the data to all my friends and close relatives. Unless I transfer over x amount of bitcoin over to a bank account with XYZ id case sensitive. At first, I panicked not knowing what to do since it looked realistic, valid and because this email included an old password as proof, after realizing there was no way they could have gather this data, I copied the email-id and looked it up on my browser. This turned out to be a reoccurring email sent to many different Gmail user and many news websites and the Federal Trade Commission advised not to pay any attention to it.

The FTC further went on to explain that Bitcoin blackmail have been on a sharp increase. This scam email was on the rise back in April of 2020 due to a data breach, and because of this, scammers took advantage of it and scammed a lot of users.

From an ethical standpoint this is unreasonable, the blame is on the company that had the data breach. It is up to the company’s security which failed because of the lack of security around our email-id, but this also included an old password which is very damaging for some people, because they might not have changed their password, or they follow the same pattern as the password that was leaked. In the hands of wrong people, they could back track or guess the current password and get into accounts. After getting this email I updated my accounts. So, any time I try to get into my account, the account needs permission from my mobile phone, much like DUO, to get into my account.

Another reoccurring phishing scam that I get at least twice a week are auto warranty scams. These are very persistent now matter how many times I block the number that is used to call me there is a new number that takes its place and calls me. These types of calls include renewing my warranty or policy, but these calls are the least convincing type of phishing due to the automated or pre-recorded. The call usually asks for personal information which could be easily used to steal my identity which includes specific information about car or my social security number.

The Federal Communications Commission has put that these “robocalls” were on the top of unwanted call complaint filed by people in 2020 and followed it through 2021. The FCC also states that these types of scams are very hard to differentiate from legit ones due the scams outputting specific information such as the specific car you own or the type of warranty you own which often makes you think these are legitimate calls.

The FCC further puts out steps that can be used to protect yourself, which I think is common sense, which includes not giving out personal information such as a social security number, credit card information, you license number. In other words, not giving them information that can be used to steal your identity. One easy way to differentiate is by looking at the caller ID because legitimate telemarketers are required to display their phone number with their name and the company they are representing.

Another dangerous type of phishing scams are ads and links that are disguised as one thing but is a link to a malicious site that could lead to your computer or phone to be corrupted by the many different types of scams out there. On a daily basis I visit questionable sites that hold whatever information/media that I use and on a daily occurrence I see ads, scams and other types of malicious links being more and more convincing. One example is when I used one of those “questionable” sites on my phone and there was an ad that mimicked a notification banner that pops down when you receive a text message or any other types of notification. This banner mimicked an Apple phone’s text message banner.

If not for the quiz and the lecture I took in class I would have clicked on, instead I hovered over it (in this case had to hard press on it). Unlike the display which portrayed a person under the Addy send me a text around the lines “I would like to meet you tonight” the link which it would send me too was an entirely different site, when I looked up the link online it was a Russian company. These are one of many types of phishing scams I have seen over the years.

Another more recent call this I found the scariest and most convincing was from a program/person portraying themselves as border patrol agents. This was even scarier for a person like me who is an immigrant. As it went on, the supposed border patrol agent said that they had found a shipment of drugs and it was under my name. Then the border patrol agent prompted me to click numbers and next to give personal information. At this point there were many red flags, one the agent did not give any information about themselves, like a name, their division or their badge number. Next was if I was indeed a drug dealer, they would not be calling me, instead I would be in cuffs being escorted my FBI agents because it is under the FBI’s jurisdiction to arrest people across states and not a border patrol agent. This just goes on to show how smart phishing scams are becoming. If I did give this supposed border patrol agent my personal information this could have led to my personal information stolen or worse being falsely accused to an actual crime that I supposedly committed.

Another topic that brings up the topic of privacy issues is organizations collecting information about web browsing information. I have seen this across many varieties of places where in some places they ask before we even do anything on the website. Which is usually displayed as whether I accept cookies or not. There are other places that automatically do this without the option first given to you like YouTube, snapchat, and other popular social media.

The most conflicting part of cookies, or other browsing collection is that you cannot access that medium of internet at all. For example, once you go into your browser and block all cookies the popular video streaming site YouTube signs me off my account, and when I go into sign back in with cookies disabled it states that google will not let me sign back in until I enable cookies.

One of the articles reviews I did on privacy focused on Facebook’s incident with their own mishandling of user’s data that was collected by third-party organizations thru Facebook. This lawsuit is a active suitcase. This is from the research I did with article review 2, were Cambridge Analytica, a data firm with their access of PII. This data was harvested when Cambridge put out a personality test called “OCEAN”. This project consisted of a series question which led to the build of psychological profiles on users and collected personal data do the users’ Facebook friends via Facebook’s platform. This led to Cambridge Analytica to provide analytical assistance in the 2016 election campaign of Donald Trump.

This is a serious violation of the use of users’ data, not only from Cambridge Analytica but with Facebook as well due to the data leak which left many users vulnerable. Tests have also shown that due to Cambridge using the data they had harvested from their tests and their link with Facebook, led to the votes to sway and led to many users reconsidering their choices.

This is just on of the few ways our web browsing data has been used in a way we, users, would not expecting to be used. For example, Google has been openly colleting users’ data collected from varies arrays of mediums, apps and sites alike. With the data they have collected and manipulate the types of ads that you come across. In other words, they sell you data to ads which you see often.

Another type of way I personally have seen browsing data been used questionably was when I first got into financial services, in other words stocks, crypto. Due to lack of knowledge, I had, I browsed the internet for advice. After looking around for a while I found one website that suited my interests but had to create a account on the website which I did. But, immediately the google account I used to create an account in the website got flooded with information from sites which I had not subscribed to. There was one thing they all had in common which was they were all financial related, and no matter how much I unsubscribed to sites which I did not even know was subscribed to my email got flooded with more emails. This is a clear violation of the use of my account, because one site basically sold my information to another site.

The collection of data is not always bad, as with all technology the reason for its existence is to make life more convenient, I even have a 5-minute speech about how software make life more convenient but because of this there will always be an underlying risks, dangers, and security issue with it. So, with the collection of web browsing data as much as the risk, there are also benefits that makes the users’ lives more convenient. This is shown at its finest in YouTube video recommendation, Tinder matching you with a likely partner or Snapchat clips. There always will be a risk to anything and everything humans use.

Finally, the topic of identity theft plays a big part of now and it will get bigger in the future. Before, identity theft went as far as just being another person on social media, or stealing credit card info, simple things. Now due to the rapid growth of technology, high-definition cameras and online presence, a malicious person could recreate an entire person itself with deep fake technology. As seen in a viral Tik-Tok video where a person mimicked Tom Cruise in videos doing everyday things.

Another place I saw deep fake being used to its full power was in the movie Red Notice 2021 which starred Gal Gadot, Ryan Reynolds and Dwayne Johnson. This movie is about art thieves and trying to steal 3 Egyptian eggs was supposedly gifted to Cleopatra by Caesar but was lost. The deep fake technology was used to break into a vault owned by a notorious collector. But this vault had a series of locks, which included an Iris scan, a voice pattern recognition, face recognition and fingerprint scan. So, they used deep fake technology to get into the vault. This is the danger that we face, even with all the biometric security that we think will keep us safe, with the right camera, the volume of pictures that can be found on the internet and deep fake technology they could become you online.

As we have seen today, technology was made to make people’s lives more convenient, which they do most of time, but this also leaves a person wide open which makes you very vulnerable. Just like with all those face filters we all use daily; deep fake technology will also be like that in the near future.

The Evolution of Malware in our Century

Malware will always be a part of life as long as we keep using technology, just like every other thing on the planet we use to live. (Food – can be used for healing but there is poisonous food as well) And just like with everything else malware has also evolved. In the past twenty years we have seen various types of malwares. In the year 2000 we saw the popular ILOVEYOU worm, which was an email that was nest approximately 50 million computers with the subject like “ILOVEYOU”. This worm caused approximately more than $5.5 billion in damages globally. Another similar malware that was sent through email with a click bait was going around in 2001 called Anna Kournikova Virus which was also an email which had the façade of containing attractive female tennis players’ pictures, but a malicious malware was hidden.

In 2003 came a very different type of virus, which unlike the other faster and more specific. This was called SQL Slammer Worm, which is one of the fastest spreading worms of all time. This worm infected approximately 75,000 computers in ten minutes. Its effects included denial of services which slowed the internet traffic worldwide. Another notable malware, although caused little damage but was the first mobile phone virus called Cabir Virus.

Now starts the era of malware infecting PCs, the first recorded one was in 2005 called Koobface Virus. This first infected the PCs and then spread to social networking sites. This worm used social engineering and phishing to access systems and steal data. Another first worm which was the first of its kind was the Conficker worm from 2008, which was a fast-spreading worm that targeted a vulnerability in Windows OS of that time, it infects a computer and disable important security features, disables automatic backup settings, and opens connections to be able to receive instruction from a remote computer.

But as malware got traction, rather than individuals criminal organizations and other organizations started to sanction teams to create advanced malware with evasion tactics that was able to outsmart many anti-malware systems. This movement began to gain popularity from 2010.

One virus which is the most recognized and still well studied malware was the Stuxnet Worm in 2010. This was most sophisticated worm which was one of the first ever created and developed by a team which is also considered as a terrorist attack. This worm’s purpose was to attack the Iran’s nuclear program and be able to manipulate not only the software but the hardware as well.

One of the first successful botnets was called Zeus Trojan whose source code was released to the public by the author in 2011, this botnet impacted millions of machines and was often used to steal banking information keystroke logging and form grabbing. Another one off the earliest type of malware was released in 2013 which was a ransomware program called Cryptolocker this malware infected computers and restricted access to it by encrypting its content. As the name portrays, to access the content on your computer you had to pay a ransom to have it decrypted and recover their files. One of the other dangerous malware that is in the ransomware sphere originated around 2016 called Cerber. This is also considered as the most prolific crypto-malware threats.

Another notable malware that was just up and coming and could have been considered as a new type at that time was the Backoff malware from 2014. This malware designed with a POS system which could be used to steal credit card information or data. Another notorious malware that used the POS system which is also called a spy ware is the BlackPOS which was also used to steal credit and debit card information. More specifically it got into a PC with stealth-based methods and steals information to send to some external servers. Some others that follow the same patterns are Chewbacca and Kaptoxa.

The most dangerous and worldwide effecting malware after Stuxnet Worm was back in 2017 named WannaCry Ransome, which I think is an appropriate name to due to it bring down major computer systems in the “Pillar Countries” like Russia, China, the UK and the US. This included locking people out of their data and then demanding ransom or have all their data deleted. The virus affected a wide array of key components that run a country, like hospitals, warehouses, banks, communications companies, and many other critical industries. This was most famously known to have breached Sony Pictures. In detail this can be considered as a worm because it spread from PCs to PCs and then once the computer’s data get encrypted the people behind it ask for ransom payments to unlock the files.

If we had though this was bad 2019 was worse, that year ushered in the rise of malware. Trickbot was a more devious trojan that has been seen in many years. If a normal PC user thinks of a more innocent or a safe and peaceful thing to do is an update, more specially a software application’s update. But this trojan disguised itself as a update with in Windows OS, more specifically a Adobe Flash Player update. After a user get tricked into downloading on of these fake updates this trojan was used to steal banking details and other personal credentials.

One of the more unique malwares that was seen in the wave that came with 2019 was called the Invisible Malware. This was a fitting name to because anti-virus software is not able to trace it at all, much less deter it. This was due to this virus residing only in memory where it cannot be traced and the only way for it be removed was to forcibly shutting down the computer.

Another malware that is unique and specific which makes it deadly in its own way. The malware called Pegasus, a Israeli spyware that attached itself to the popular messaging/calling app WhatsApp(which is very common in India) targeting Indian journalists. The malware attached itself to devices disguised as an exploit link. This led to the collection of the targets’ personal information.

As the year 2021 rolled by, so did the increase in the effectiveness of malware. One of the most notable malwares is the Mirai malware, which was also covered in class. This malware is very notable this year is because of the exponential growth in IOT devices. In other words, the smart home technology. What this malware basically does is it turns IOT devices running on Linux or ARC processors turning them into zombies. This means that this malware can take control of smart devices remotely.

Another malware uniquely suited for this year is CoinMiner. Due to rise of cryptocurrency in 2020-21 this is a trojan horse that infects the computer’s resources to mine digital currency without the users’ permission.

Over a twenty-year period we have seen the range of evolution that malware has gone through. From the iconic ILOVEYOU worm which was basically a click bait email to the Mirai malware which basically turn smart devices into zombies. The development of these malwares has kept up with the pace of development of new technology.

The biggest headache I personally think that is faced by the security community is the effectiveness of the malware that is being developed. What I mean by this is that this is no longer a problem that can be fixed by anti-malware software due the specificness of the malware, like the Pegasus virus discussed above. I also did a article review discussing polymorphism and detecting DCOs.

Another biggest hurdle that the security committee is going to face is the degree of naiveite of the lack of knowledge with users when it comes to this issue. Technology is everywhere now, and I mean everywhere from you bed, to the toilet seat you, to the things a patient might use to stay alive. Before it was all done locally, now this all connected to a cloud, or the internet which make these more vulnerable than it was when it was local. Now the issue of naivete place a big role, Me and my groups did a presentation on cyberattacks on health care and I was very surprised to the extent of the naiveness to the point it feels like they do not care about he patients at all. Most hospitals have shown to still be using Windows XP! Most kids today have never used that OS or even heard of it on top of it being old Microsoft itself has dropped it and does not update that version. Just imagine the number of vulnerabilities it has, and hospitals have been putting all their patients online. This is a serious problem.

The naiveness part stems from the lack of knowledge. In my opinion school should adapt their educational curriculum to include this topic because this as important to learn as safe sex and other critical common-sense knowledge. As I have said above we use technology the majority of our day and night if not 24-hours 7 days a week. This is not where it ends technology will not stop all of the sudden it’s a exponential thing with no end as long as we humans are alive and to not know how to protect ourself against malware is absolutely naïve.

The main reason why the population of malware authors have evolved, and increased is because of how easy it is. Just like from the dawn of time humans always do what is the easiest and most beneficial. In this era a malware author reaps money. Because of the lack of programmers in the other side or playing defense, companies often pay the ransom from the ransomware attack, hackers can get into companies and access their data due to the lack of development and resources.

But just like with the growth of the threats from malware, so have the solution. There are many solutions out there to combat malware, one solution I covered in an article review when there is DCO attack to perform a static analysis of the DCO code and the finding patterns behind the files. Simple solutions like help, but only of a limited time until hackers find their way around this as well.

What I think will be the best solution to stop most of these attacks before it even happens with simple things like follow protocols. Update your system whenever there are updates available. Don’t fall for phishing scams that will open up a port of hackers to get into your systems. Don’t visit questionable sites, first do your research before going into those sites. Keep updating you passwords not follow the same pattern keep changing it. Due to IOTs your PCs and other things are connected as well through your internet router so secure your PCs as much as possible.

There are many ways you can protect yourself, but people still fall victim to these malwares. Partly because of the ever-growing range of malware and partly because people are lazy or do not have the knowledge for this.

Throughout this essay we saw the many varieties if malware, how it has evolved over just 20 years. Then we looked at why malware is on the rise and how to protect yourself against it. The phrase “knowledge is power” is very true in this situation. Just like with many things where you need to know the dangers, like when one gets a driver’s license, they go through how to properly use and how to not use. If used in the wrong way, the dangers are deadly. So, why should technology be any different, in order to use it you need to learn both sides of it to use to the maximum extent and protect yourself.

Works Cited

Rankin, Bert. “A Brief History of Malware—Its Evolution and Impact.” Lastline, 14 May 2018, [www.lastline.com/blog/history-of-malware-its-evolution-and-impact/](http://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/).

“IoT Security Issues in 2021: A Business Perspective.” Thales Group, 2021, www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats.