On-Line Attacks

Areej Manzoor

I.T Webtech

Mrs.Bohuslov

12/3/17

When it comes to the internet, there are a lot of dangerous out there that can occur. People might hear on the news that a celebrity's social media got hacked or that a hospital or bank’s security networks got breached and that every patients or clients personal information has been stolen . People hear these things everyday, but they don't think to themselves that this can also happen to them. Sadly, anyone can be targeted. Typically people don't know what to look out for when it comes to the dangers and threats of the internet. As the technology enhances, there are many threats out there that are producing more and more dangers. How can one identify these threats and stop them?

One of the common cyberattacks that can happen to an individual is Password Phishing. Roughly around 60 to 70% of an individual's email is spam. Most of spam is harmless, but there are others that can contain viruses. Those links can make people give out their private and personal information in order to hack them, this is the most common mistake a person can make. Luckily anyone can get rid of spams can clean their inboxes by installing vendors and anti-spam softwares and programs. You can also install anti-phishing programs in case that if you're stuck with an password combination for more than one system. Also the best way to avoid password phishing especially on your cellular device such as iOS; is don't enter a password when a pop-up screen appears from a third party app. It is easy for someone to make an app that looks like from your system, asking for a password. Be cautious of what apps you download on your device; especially on iOS. These hackers tend to gain information on you iCloud or you In-App purchases that they can easily steal. The best way to identify a phishing attack on iOS is that if it closes the app and it has some sort of dialogue, then it's easily identified as a phishing attack. It may look like it's from your system, but if you see its functions very closely, you can tell that it's a phishing attack.

There are smart people out there who do have firewall programs and have anti-virus software to protect themselves from the threats and dangers. However the biggest and most common mistake a company or even an individual can make is not updating these softwares frequently. These programs and softwares are always creating patches and they are always notifying an individual with updates. If a company or person does not update these programs frequently, they are easily penetrable and vulnerable. There was an article that stated that this million dollar company was hacked and all information was stolen from them. They had a very strong and sufficient firewall and they had anti-virus softwares. The reason why they had gotten hacked was because they didn't update these programs when there was many patches made to destroy the virus that attacked them. Sadly they didn't update them and this was how the company “crashed” down. These programs do come with alerts and notifications that they have an update and when it's possible, people should come through and update these as fast as they could. When updating these softwares they have a better and more efficient way of protecting them from cyber attacks. After all, new threats are emerging everyday and all you really have is your firewall and anti-virus softwares to protect you. Hackers can also hack into these softwares and make sure that a person does not receive a notification or alert that they need an update for the program. To be more alert and cautious, just in case a person is feeling paranoid, check on updates frequently and verify and make sure that they have the latest update installed in order to have a more efficient and strong software when it comes to updating the firewall and anti-virus softwares.

Most people around the world use social media, it's become our outlet to escape the real world and head to the virtual world. People enjoy sharing to the world what experiences they had made. Its one of the best way to communicate and find our friends. Unfortunately it's one easy way hackers can spread cyber attacks and viruses. However hackers have used this to their advantage. Catfishing is not compared to what hackers do in the online world of social media. Social media threats in cyber attack start out as a strange friend request an individual receives. Sadly there are people out there who let these hackers into their social media and letting them see what they post online. First things first; don't accept requests from people you don't know, this protect you and doesn't allow hackers to see what you are doing. Especially when it comes to a company's social media account, hackers love to see what they can expose. Notorious hackers always start out as social media threats and move on from there. Many hackers create fake accounts in order to request a friend request. Its very easy to target fake accounts, but the best way to avoid them is declining friend request of people an individual does not know. One of the harmful social media threats is Site Compromise. Site compromise is when a hacker compromises a sites code and if any user who decides to go visit that site gets attacked. Unfortunately hackers have also discovered that they can do this to advertisements and they can create rouge-third party applications. Hackers have come up with a way to shorten the URl so it's difficult to tell if the link is legitimate or if it seems suspicious and sketchy. This makes it easier for the hacker to gather up personal information from the individuals who had visit the website that has been compromise. The best way to avoid this is be cautious on what websites a person is going on. It's easy to see a mysterious link and evaluate if it's some sort of virus or a legitimate website, be smart on what links are sent to a person and see if it's sketchy.

Hackers can easily disguised themselves as nothing but harmless links or websites. Unfortunately there is a cyber attack called IP spoofing which sadly, does that. IP spoofing is when a hacker creates a harmless host to disguise his identity, create or spoof a website to get into its network. The hacker gains the IP address of a host and changes it in his/or hers way. IP spoofing basically takes over a browser. A user who wants to visit the website will see the URL and think it's not harmless. For example let's say a user wants to go to www.youtube.com. The hacker who is doing the IP spoofing can create something alternate to youtube, but the link address will be the same. When the user clicks the link or presses enter, what will pop up is the content that the hacker had decided to make. If the user sees active or dynamic activity on the content and interacts with it, this makes it easier for the hacker to steal and gain information and personal information from the user. Depending on the website; say Bank of America, they can also steal sensitive data such as credit card numbers or passwords. If they were more malicious they can also install malware. The hacker can also take control of the compromised computer and they can also send out numerous numbers of spam. One of the ways a person can prevent from being IP spoofed is if they use an access control list to deny private IP addresses on your downstream interface. They can filter out which Ips are good and which ones are suspicious or sketchy. Another brilliant way to make sure a person can prevent from being IP spoofed is to get spoofing detection software. It is a good idea to get something to alert you if you’ve been an intended victim of one. Luckily, there is an abundance of software out there that can help you with this issue. One great software or program that can help you detect IP spoofing is Xarp. This program alerts you if you have been in a serious case of IP spoofing. Xarp also detects other spoofing material, not just IP spoofing, better to be safe than sorry.

One of the worst attacks that can happen to an individual is Sensitive Data Exposure. Sensitive data exposure is when an application does not efficiently protect sensitive information or data. This could be a wide range of data, from passwords, to credit card numbers and even health records. A scenario of this could be if an individual accidentally uploads a set of data somewhere. An attacker can easily read this data and can hijack or compromise the data, and it could turn out to be horrible. How does an individual prevent this from happening? One of the best ways is to make sure they had encrypt all sensitive data so it's harder for the attack to read the material. Also be sure that strong encryptions,algorithms, and keys are used for the sensitive data. Lastly; don't necessarily save sensitive data. The less of the important and sensitive data, the better!

It is important that each individual and company knows what security and cyber attacks are out there. People think to themselves that this could happen to them. These attacks just target individuals that know nothing about the threats that have been made. Almost every day new threats are being created. The best way for people to protect themselves is to know what threats are there and how to stop them. The most smarted way is to install firewall and anti-virus softwares and make sure to update them frequently. As the technology enhances, there are many threats out there that are producing more and more dangers. Its important that people should educate themselves about the threats and how to protect themselves.

Citations:

Top seven social media threats,Shantanu Ghosh,ComputerWeekly.com, September 12 2017

PSA: A new phishing attack could trick you into giving away your Apple ID password, Chance Miller, October 10 2017

The 5 cyber attacks you're most likely to face, CSO Online, Rodger A. Grimes, August 21, 2017

OWASP TOP 10: Sensitive Data Exposure (#6), Detectify Blog,November 01, 2017

What is IP spoofing (IP address forgery or a host file hijack)? - Definition from WhatIs.com, SearchSecurity, November 03, 2017