International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:3, 2015

Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users

Haydar Teymourlouei

***Abstract*—**It is important to take security measures to protect your computer information, reduce identify theft, and prevent from malicious cyber-attacks. With cyber-attacks on the continuous rise, people need to understand and learn ways to prevent from these attacks. Cyber-attack is an important factor to be considered if one is to be able to protect oneself from malicious attacks. Without proper security measures, most computer technology would hinder home users more than such technologies would help. Knowledge of how cyber-attacks operate and protective steps that can be taken to reduce chances of its occurrence are key to increasing these security measures. The purpose of this paper is to inform home users on the importance of identifying and taking preventive steps to avoid cyber-attacks. Throughout this paper, many aspects of cyber-attacks will be discuss: what a cyber-attack is, the affects of cyber-attack for home users, different types of cyber-attacks, methodology to prevent such attacks; home users can take to fortify security of their computer.

***Keywords*—**Cyber-attacks, home user, prevention, security, technology.

I. Introduction

CYBERattack is a big issue that needs to be focus in depth because of the wide-spread use of the technology. The growth of technology is accompanied by cyber security threats or "cyber-attacks" which threaten home users security when using such technologies. Cybersecurity involves protecting that infrastructure by preventing, detecting, and responding to cyber incidents. Unlike physical threats that prompt immediate action–like stop, drop, and roll in the event of a fire–cyber threats are often difficult to identify and comprehend [9]. Private data is being exposed due to the growth of cyber-attacks which inflicts negative impacts against usage of technology. Technology may serve as convenience for most home users however; dangers incurring from cyber-attacks that come with the technology can have the same impact negatively. Many home users may not be aware of the danger of cyber-attacks, a lack of knowledge in the subject can lead to many home users falling victim to cyber-attacks.

An important component to prevent cyber-attacks is to understand what a cyber-attack is and why it is important to protect against it. The probabilities of being targeted by cyber-attacks are high and bound to increase with the use of internet. Cyber-attacks are more of an umbrella term which covers various different methods for others to cause malice over the internet. A cyber-attack is when someone gain or attempts to gain unauthorized access to a computermaliciously damagingsystems, or stealing valuable information from that computer.

Cyber-attacks are sent from one computer or network to another with the intent of compromising the target computer or network. Cyber-attacks cause security concerns for using the internet safely considering the adverse outcomes of such attacks.

Cyber-attacks are dangerous due to their ability for one to occur against a victim who could be across the globe. This allows for the growth of cyber-attacks to continue generally untamed and difficult to trace. Cyber-attacks cannot be stopped completely, due to the fact that new exploits are discovered every day. However, there are plenty of steps users can take to deter cyber-attacks. Some of these steps include: installing firewalls, keeping software up-to-date, ensuring infected machines are not connected to others, and data encryption. These extra tips will provide clarification and can be a great resource for any home user. All of these steps will be covered in the quick reference guide.

II. Discussion

A. The Impact of Cyber-Attacks on Home User

There are multiple questions a home user could commonly ask about the subject of cyber-attack. What is a cyber-attack? What can be done to protect myself from such an attack? How will I know if I have been a victim? Home users are often depicted as the most vulnerable and susceptible to cyber-attacks. Since home users are usually the least educated about cyber security; cyber-attacks have much more success targeting home users. Cyber-attacks can consist of spreading malicious code like viruses, stealing personal information using phishing and spam, and many more tactics. Cyber-attacks can lead to fraud, identity theft, and many other crimes which do not need technology to occur. One important concept that any home user should understand is that any computer connected to the internet, can be susceptible to cyber-attacks.

It is up to the home user to take necessary steps to protect their computer from cyber-attacks. Since we live in a new era of technology, much more private information is being stored in computers and networks. Computers are used daily; people use computers for: shopping, sending e-mails, education purposes, entertainment, and productive purposes. Every single user will come across some kind cyber-attack, considering the inability to stop all possible attacks. Educating home users will not only increase security against cyber-attacks but allow for the development of new security measures as well. Computers do not come adequately

Haydar Teymourlouei is with the Computer Science Department, Bowie State University, Bowie, MD 20715 USA (e-mail: hteymourlouei@bowiestate.edu).

equipped with enough software and information to effectively protect from cyber-attacks on its own. The home user's awareness and sense of responsibility is necessary in protecting against any cyber-attacks. After home users are well informed with the types of cyber-attack threats, and methodology to prevent such attacks; home users will be less vulnerable to such attacks.

B. Different Types of Cyber-Attacks

It is important to understand that there are always possibilities for new methods of cyber-attacks to be discovered. In order to limit these attacks, comprehension of current methods cyber-attacks use must be understood. Cyber-attacks continue to increase untamed due to the ability of remote attacks. Remote attacks are common among cyber-attacks due to the possibility of successful attacking any computer from anywhere across the globe. Once one comprehends the different types of cyber-attacks; there are various ways to protect home users from cyber-attacks. All of these different types of cyber-attacks can be countered with some preliminary steps.

1. Malware

Malware is known as any computer code created for causing malice [5]. Although one may not have known the technical definition of malware, chances are the user has fallen victim of some type of malware. Malware is capable of infecting computer systems slowing or shutting them down and steal valuable information. Malware continues to grow limitlessly along with cyber-attacks and is a popular tool in cyber-attacks. Another problem with malware is the contagious abilities of it. Malware is able to quickly spread across the web since due to its ability to be a small file with capabilities of infecting whole file systems. Malware can cause more harm the longer it exists in the home users system. For this reason it is important to protect against, detect, and eliminate malware from home user's computers. Malware has three common forms:

a. Spyware

Spyware is the most common form of malware for stealing valuable information. Spyware simply does as the name implies and spies on any information home users enter in the computer or browser through various methods [5].

b. Viruses

Computer viruses are similar to biological viruses in terms of survival. Biological viruses need to feed off of a host through the host's cells to live. On the other hand, computer virus, files in the computers system are essentially to the "cell" inside of the computer host. Depending on the severity of the virus, infection can spread to system files effectively slowing or even damaging the computer entirely [5].

c. Worms

Worms, although much less common can be more of a threat due to their ability to live on their own. Worms work similar to ways a virus works except worms do not need a host to live. This is dangerous because without the necessity of a host, infection can spread much quicker. Worms can also be harder to detect due to the fact that no host is needed [5].

2. Password Attacks

As computer users, passwords serve as essentially keys to all our private information. When the password is lost, it must be retest quickly to prevent the risk of theft. For such reasons, it is important to understand how hackers can essentially steal passwords from unsuspecting victims. Some methods of password attacks include: password guessing, password resetting, and password capturing. Password guessing is predicting possible password combinations until the right combination is found. Although this method may seem to take unreasonable lengths of time to accomplish, software's can shorten the process. Since many people still use common passwords such as their birthdays or names for passwords; the process is much shorter than many may think. Another threat is reusing passwords, essentially allowing hackers to access multiple accounts using that one password. Password resetting is not a very common method of password attacks. It requires the hacker to get access in to the file system of the operating system before anything can be done. However, once inside, hackers can modify and crack system files which contain the user's password. Finally, password capturing uses malware which allows hackers to unsuspectingly track all of user's keystrokes. This effectively allows hackers to get the user's passwords right away.

3. DDos Attacks (Distributed Denial of Service Attacks)

A DDos attack is used to hack websites and companies data servers. According to Dan Stone, these attacks work based around the principle of overloading a computer system or server. Overloading the system leads to slowing down or even shutting down servers entirely [8].IfDDos attacks issevere enough it can be used as a distraction from other security vulnerabilities which can lead to stolen information. A good example is how a small DDos attack took place against some banks which disguised the even bigger security breach hackers were able to exploit, leading to fraudulent money wiring [4]. Users should be notified immediately if a company trusted with that user's information is breached. The problem for users and DDos attacks and companies getting breached is the idea that users cannot do anything to stop it. Although in theory users cannot stop these attacks, something can be done to limit the damage.

4. Pop-Ups

Pop-ups are a major component and common feature of web browsing. Many reputable organizations use pop-ups for multiple different purposes. However, cyber-attacks have occurred where the hackers generate a fake pop-up which can appear even if a reputable companies' website is being browsed. An example of a malicious pop-up is if antivirus software is out of date home users who are not educated about the potential dangers of these pop-ups may be tempted to download the software. Installation of this software can lead to malware being able to directly infect the home user's

computer. It is important to never trust any suspicious looking pop-ups. Looking at the URL of such pop-ups generally reveals whether the source is genuine or not. Pop-up blocker software is highly recommended for any web browsing. Many common web browsers include pop-up blocker software automatically for convenience and added security while browsing.

5. Software Updates

Cyber-attacks commonly exploit security holes in software to gain access to home user's computers and steal valuable information stored by such applications. Since software companies cannot patch every single possible exploit, updating software is essential. Software update patches previous exploits in older versions of the software. These updates are free and many applications include an updater can inform home users about when a new update is available. Updating software also fixes problems with the program and usually increases the software's stability. Many operating systems even include updaters which can update multiple different applications simultaneously. Although even up-to-date software can be exploited, chances of exploitation greatly decrease.

6. Public Unsecured Wi-Fi Network Attacks

Public Wi-Fi networks are generally seen as convenient to most home users. Public Wi-Fiis common in restaurants, shopping centers, airports, and many other places. These public networks are convenient however; public networks are not password secured. Public networks are at much greater risk for cyber-attacks then networks which are private and password protected. Cyber-attacks can target these networks and monitor or steal valuable information sent over these networks.

7. Phishing Scams

Many people use e-mail have probably received e-mail of some ridiculous lottery winning from other countries or various others scams asking for personal information. Phishing are fake emails made to look legitimate asking for information for malicious purposes [3]. These types of e-mails are sent to usersto get trap in scams by giving away their information to scammers. These e-mails can come from a wide range of fake sources including lotteries, and even "banks" asking for confirmation of personal information. Phishing e-mails is dangerous as they trick the home user into giving personal information away without the use of malware or any other virus.

8. Man-in-Middle Attacks

Whenever information is shared over the internet; it is transported through multiple networks before reaching its destination. A Man-in-Middle attack intercepts the data as it is going through these various networks. These attacks can be very difficult to detect as it is still possible for the data to reach its destination. Hackers can simply copy the data being sent to a separate network of their own without interrupting the path to the original destination. These attacks can be very dangerous due to their ability to go undetected to novice home users.

9. Eavesdropping

It is an unauthorized real-time interception of a private communication, such as a phone call, email, or videoconference. Unlike the Man-in-Middle attack, eavesdropping simple monitors the information being sent from the client to the server. Information is not sent to another computer in the case of eavesdropping. Many home users may not be able to realize whether a network connection is being eavesdropped however; there are precautions to limit the chances of such an occurrence. For example, only send information through servers which are certified as secure. Make sure computer doesn't have any unknown service or any ports open that are not being used.

10. Session Hijacking

Session hijacking is a type of cyber-attack in which a valid session between a client and a server is temporarily used, thus giving the name "Hijacked" for malicious purposes. This works by way of using the valid client's cookie which is authenticated by the server to connect to the server. Once a valid connection is established the clients information transferred to the server can be accessed. Ensure the reputation of the company receiving the information, as well as checking server security for proper certification. Giving information to servers without checking these simple prerequisites can lead to almost undetectable information loss.

III. Methodology

In today's technology driven world, cyber-attacks are more active than before and putting the average home user at risk. There are many different ways for one to protect information from cyber-attacks. Maintaining computer privacy takes a multi-pronged approach. It can be challenging for home users since they don't have much knowledge about cyber-attacks. The quick reference will give more in-depth tips on how to protect your information and significantly reduce the chance of such cyber-attacks.

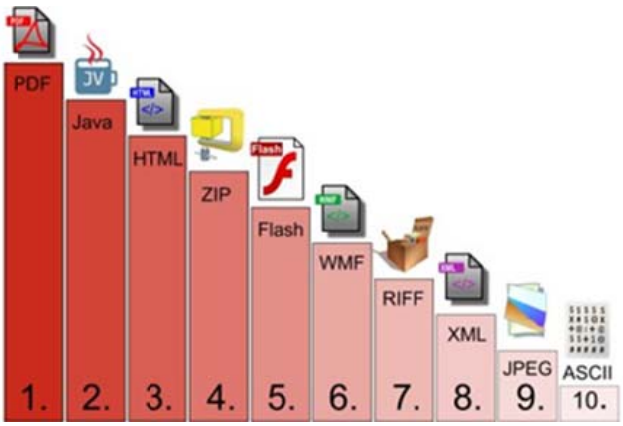

Fig. 1 AVTEST Report

According to AVTEST, after long-ten years of study the researchers have concluded that these are the top 10 list of most infected file types. As mentioned in the report majority of the vulnerabilities in computers are due too: Java, Adobe Reader, and Flash. About 66 percent of the exploit versions were recorded between 2000 and 2013 [7]. Since home users do not update their machines regularly therefore they should pay more attention to these software's updates regularly.

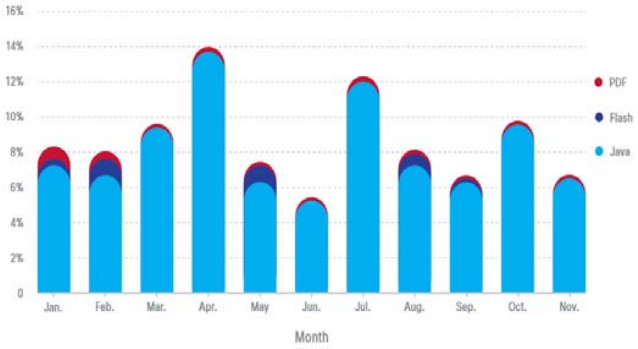

Fig. 2 Malicious Attacks Generated through PDF, Flash, and Java 2013 [2]

According to Cisco 2014 report, out of all the web threat Java software continues to provide the highest vulnerability to give the chance to hacker to exploit user computer. The two other most popular vulnerabilities detected are: Flash and Adobe PDF document which is used a lot by home users. For threats such as Java exploits, the most significant issues facing security practitioners are how malware enters their network environment and where they should focus their efforts to minimize infection [2].

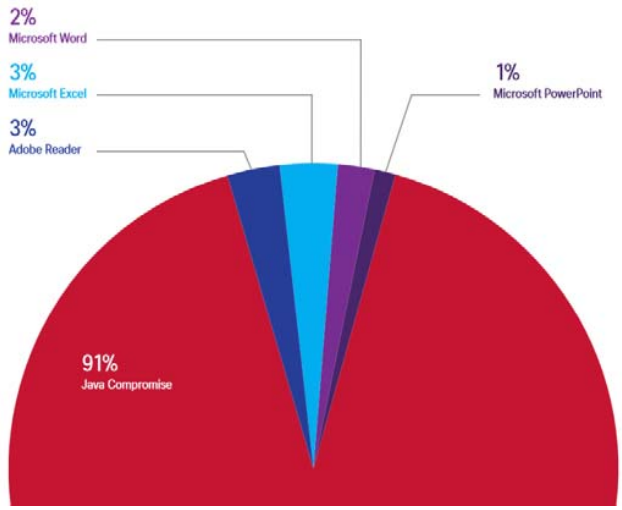

Fig. 3 Indicators of Compromise, by Type [2]

This diagram is also part of Cisco 2014 report, states what type of software caused the compromise to the system. 91% of the malicious attacks were generated through Java since it can launch an executable file that can run malicious events. As is indicated in the report, the ubiquity of Java keeps it high on the list of favored tools for criminals, which makes Java compromises by far the most malicious "chain of events" activity in 2013. As Java's "About" webpage explains, 97 percent of enterprise desktops run Java, as do 89 percent of desktop computers overall in the United States [2]. There are other software's that compromise and vulnerable to computer security: Microsoft word, Microsoft PowerPoint, Microsoft Excel, and Adobe Reader as shown in the diagram.

IV. Quick Reference: Guide to Prevent Cyber-Attacks

In this digital era and increase use of the technology makes it tremendously important to secure our data/information. More data is being transmitted over network and stored in computer today. It is very beneficial to be educated and use tools to prevent from such cyber-attacks. Although cyber-attacks cannot be stopped completely; their effectiveness can be limited. Following the steps given will give a much higher level of security for valuable information.

1. Choosing Strong Different Passwords

The importance of selecting strong password cannot be emphasized enough since it's a key to the private data. It is essential to use different passwords for different accounts. When someone uses the same password for all accounts, if that password were to be stolen, thieves would have access to multiple different accounts as opposed to someone who uses a different password for each account. Surveys show that 61% of people reuse the same password for multiple different sites [1]. A strong password contains at least 12 characters, which includes special character, lowercase and uppercase letter, numbers, and avoid using personal information. Although long passwords can be hard to remember; there is numerous mobile applications and software available which allows users to store all passwords in safe location. This "safe" can be accessed as long as the user remembers one master password. With such tools, users should be inclined to develop longer, complex passwords without worry of forgetting them. This will make retrieving information much more difficult for cyber-attacks. Also, make sure whenever entering a password in the browser it is secure meaning the URL starts with https instead of http.Since it is hard to remember all passwords, consider using a free password manager such as Last Pass or find others here [6].

2. Keeping Your Information Confidential

Sometimes preventing cyber-attacks is as simple as using common sense. Users need to be wary of giving out information to websites with questionable reputation. Giving up valuable information to such organizations can lead to identity theft and fraud easily. E-mail is a popular way for hackers to spread malware and trojans to a computer. One should always check the source of the organization before handing out any personal information to anyone. Whenever in doubt simply do not trust the organization.

3. Antivirus Software

The first measure step home users need to take is to protect one's personal computer is by installing anti-virus software on the system. Antivirus software is software that detects, prevents, quarantines, and removes malicious computer programs from the system. Make sure to install some type of antivirus software, allow the automatic updates to take place every day and scan the system daily. Make sure to set antivirus to scan all files types including emails and attachments. There are many different types of freeware anti-virus software which is beneficial Microsoft Security Essentials is one of them. It provides real-time protection for home users to guard against viruses, spyware, and other malicious software's. Antivirus software is essential in scanning downloaded files to ensure malware does not enter the computer. Following these steps will significantly reduce the chances of malware infection.

4. Using Public Wi-Fi

Public Wi-Fi is susceptible and convenient dangerous as well. Since public Wi-Fi is unprotected; one suggestion would be to avoid using when unnecessary. If one wishes to use public Wi-Fi connections, no information of any kind should be sent over such networks. Avoid transactions or registering for anything that requires any input of personal information. Remember to not allow any device which has been connected to public Wi-Fi networks to remember these networks. Only allow devices to connect to these networks when prompted by the user. Users need to avoid using public network and use their data or hot-spot while they are in public places.

5. Safe Browsing

One should be weary of using websites that have no security measures in place for personal information. Most websites will show links to the security certificate if information is encrypted. Home users can simply check for such certificates to assist in deciding whether the organization can be trusted with information. Here are some tips:

- Disable the use of remembering passwords for sites in all browsers
- Disable the use of remembering what entered in form in all browsers
- Make sure browser setting is set to clear data when browser is closed
- Block pop-ups for all the browsers
- Set the internet zone security level
- Do not open unknown e-mail attachments or respond to unknown e-mails
- Password protect all devices that are connected to the internet
- Do not respond to online requests for asking personal identifiable information

6. Keeping Software up-to-Date

Software updates are essential to proper security since no application is one-hundred percent impenetrable. Most software includes automatic updaters which allow updates to complete with a few clicks of the mouse. Some software even has pop-ups which remind the home user when a new update is available. If an application does not have automatic updates, users should check the website of the company which develops the software to check for new versions of the applications. Home users should set a specific time at least once a week to check for updates to every application.

7. Firewalls

Firewalls are applications that check for any information that is communicated from the user's computer with anyone else. Firewalls are guard against any unwanted communications from any source. Firewalls are an essential second layer of protection against any types of cyber-attacks. Firewalls may seem inconvenient for the reason of having to monitor all communications a computer makes. Most firewalls however, can be configured to only check communications if the source is untrusted. Home users can configure firewalls to the level of protection they want.

8. Free Software Downloads (Freeware)

Home users need to use more responsibility when it comes to downloads. Not all freeware software's are malicious however; it can carry viruses and other forms of malware along with it. Use antivirus software to scan any software download (not just freeware) in order to check whether the software should be installed. Only download freeware from sources which can be confirmed as reputable and legit. It is not advised to install freeware from an organization which is unknown. Home users should be cautious and exercise responsibility when making the decision whether they should download freeware or not.

9. Avoiding Peer-to-Peer (P2P) Downloads

P2P is when one user decides to upload a file to file sharing websites for other users to find and download. The big problem with P2P is that files uploaded by other users are not inspected for infections by anyone before uploading. This can lead to home users easily downloading malware and corrupting the computer greatly. In addition, P2P files usually contain illegal content such as pirated movies, music, programs and much more. Illegally downloading these files can lead to criminal charges and restrictions by your Internet Service Provider. The best preventive method against P2P is to not use it.

10. Back up Important Data

Computers store tons of valuable information. Computers can fail and hard drives can become corrupt which leads to endless information lost. Computers with malware are especially susceptible to corruption due to the infection of the file system. Using an external hard drive or some other storage device can ensure that when hardware does fail, important data is still safe. External drives can come in a variety of forms, prices, and sizes. Plenty of options exist for every home user to find a drive right for them.

11. Data Encryption

Files can be encrypted to ensure that if these files are to

ever fall in to someone else's hands, information cannot be read.It prevents the hacker from modifying, changing or getting access to the personal files/documents. Modern technology advancements allow whole hard drive disks to be encrypted. While most users will not need to encrypt everything on the hard drive, encrypting important files is a great security measure to ensure that if data is to ever fall in the wrong hands it is not easy to access. Home users must remember encryption is not one hundred percent secure and can still be broken. However, files with encryption are much harder to read than files with no encryption.

12. User Accounts

Many operating systems come with the ability for administrator to manage account privileges. This improves the security by limiting application software to standard user's privileges until an administrator approves it. This allow only application that are trusted by the administrator to receive privileges, a user cannot run applications without administrator grant permission. Also, make sure when in public place never leave computer screen unattended, lock or logout of the account.

13. Operating System

Software such as windows update can manage the installation of updates simultaneously for further convenience. Other OS usually include applications with similar abilities, checking OS documentation will allow the home user to comprehend where to find and how to use such software. Always set the windows updates to check and download the updates automatically. So every time the OS-vendor sends out the latest patches to known vulnerabilities it gets downloaded and install in the system.

14. Turn off Unused Services

Many programs may have services that run in the background of the computer. Some malware may also only run in the background to avoid detection. Users need to check to make sure there are no unknown or unused services running in the background. The programs or applications that are not used or needed are turned off. It will help reduce the potential harmful threat to the system as well as help enhance overall performance of the system.

15. Be Aware of External Drives

Always double check the source of external drives before plugging them into the computer. External device for the computer such as flash drives can be infected with viruses, spyware or malware. Do not plug in any external drives whose source is unknown. Putting an unknown an external drives that has been corrupted and opening any documents from that USB can automatically affect the computer. So be aware of putting or connecting any unknown external drives such as: (USB, DVD, CD and etc).

16. E-mail Security

It defends against the spams, blocks phishing, viruses, malware, protects privacy and data lost with automatic encryption. E-mail is a popular way for hackers to spread malware and trojans to a computer user. To ensure your computer doesn't get affected:

- Do not open unknown e-mail attachments or respond to unknown e-mails
- Do not respond to online requests for asking personal identifiable information
- Let anti-virus to scan email attachments prior opening
- Never open emails from spam box
- Never click on a suspicious link send in unknown email

17. Basic Security Tips

The use of technology in the area of education is becoming popular and more dependent than it has ever been since the existing of technology. By knowing and integrating online security basic not only will help users to be able to use the tools to gather information effortlessly but they will learn technical skills that will advance them in the future for their professions. The future of this world is technology dependent and it will become a problem if the future generation does not have some basic fundamental and knowledge how to prevent and protect their computer from cyber attacks. Here are some basic rules:

- Don't share their passwords
- Recognizesuspiciousactivities
- Browse safely online
- Don't leave computer unattended
- Do not type passwords on public computer
- Clear browser after leaving computer

18. How to Deal with Cyber-Attack

- Find out if your computer have some suspicious activity
- Fix the problem and try to restore the computer to service
- Unplug internet cable and shutdown the infected machine immediately
- Take the computer to a certified computer technician
- Take appropriate action based on cyber security policy

Even though you are protected there are times that intruders may still get in either through brute force or by finding vulnerabilities with the home such as an open window. Hackers look for vulnerabilities with networks and make an attempt to break inside to gain access to critical data that could compromise you or an organization. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application. The importance of the having security on a system is to prolong hackers from actually getting and breaking into the system.

V. Conclusion

In conclusion, it's very essential to educate home users on how to make better decisions and understand the risk associate with cyber-attacks. The key to deter cyber-attacks, with the

information given we as a whole can reduce the effects of cyber-attacks. Governments across the globe need to take legalaction and enact laws to protect citizens from these threats. The threat of identity theft and fraud is severe enough to warrant the necessity of educating every home user. If the effects of cyber-attacks are not at least contained partially; these threats have the capability to undo all the positive impacts computer technology has on society. Cyber-attacks are always changing and new methods can always be discovered. However, this should not deter users from at least enacting some steps to protect valuable information. User's knowledge, awareness and responsibility are the best defense against any kind of cyber-attacks regardless of government action. There are many different ways to protect data other than just the methods given. Being informed about these threats will hopefully reduce chances of such threats or even encourage others to discover preventive methods of their own.

REFERENCES

[1] CSID. (2012, September). CONSUMER SURVEY:. Retrieved from CSID:http://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf
[2] (2014). Cisco 2014 annual security report. Retrieved from http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[3] Indiana University. (2014, November 12). What are phishing scams and how can I avoid them? Retrieved from Indiana University Knowledge Base: https://kb.iu.edu/d/arsf
[4] Musil, S. (2013, August 21). Cybercrooks use DDoS attacks to mask theft of banks' millions. Retrieved from CNET: http://www.cnet.com/news/cybercrooks-use-ddos-attacks-to-mask-theft-of-banks-millions/
[5] Pennsylvannia State University. (2013, March 14). Types of Attacks. Retrieved from Pennsylvannia State University Personal Web Servers: http://www.personal.psu.edu/users/j/m/jms6423/Engproj/Types%20of%20Attacks.xhtml
[6] Schwarz, C. D. (2014, December 26). 5 ways to prevent a personal cyber attack. Retrieved from http://hereandnow.wbur.org/2014/12/26/cyber-security-sony
[7] Selinger, M. (2013, 12 04). Adobe & java make windows insecure. Retrieved from http://www.av-test.org/en/news/news-single-view/adobe-java-make-windows-insecure/
[8] Stone, D. (2015). Detecting Cyber Attacks. Retrieved from Everyday Life - Global Post: http://everydaylife.globalpost.com/detecting-cyber-attacks-30915.html
[9] U.S. Department of Homeland Security, Federal Emergency Management Agency. (2013). Cyber attack. Retrieved from website: http://m.fema.gov/cyber-attack