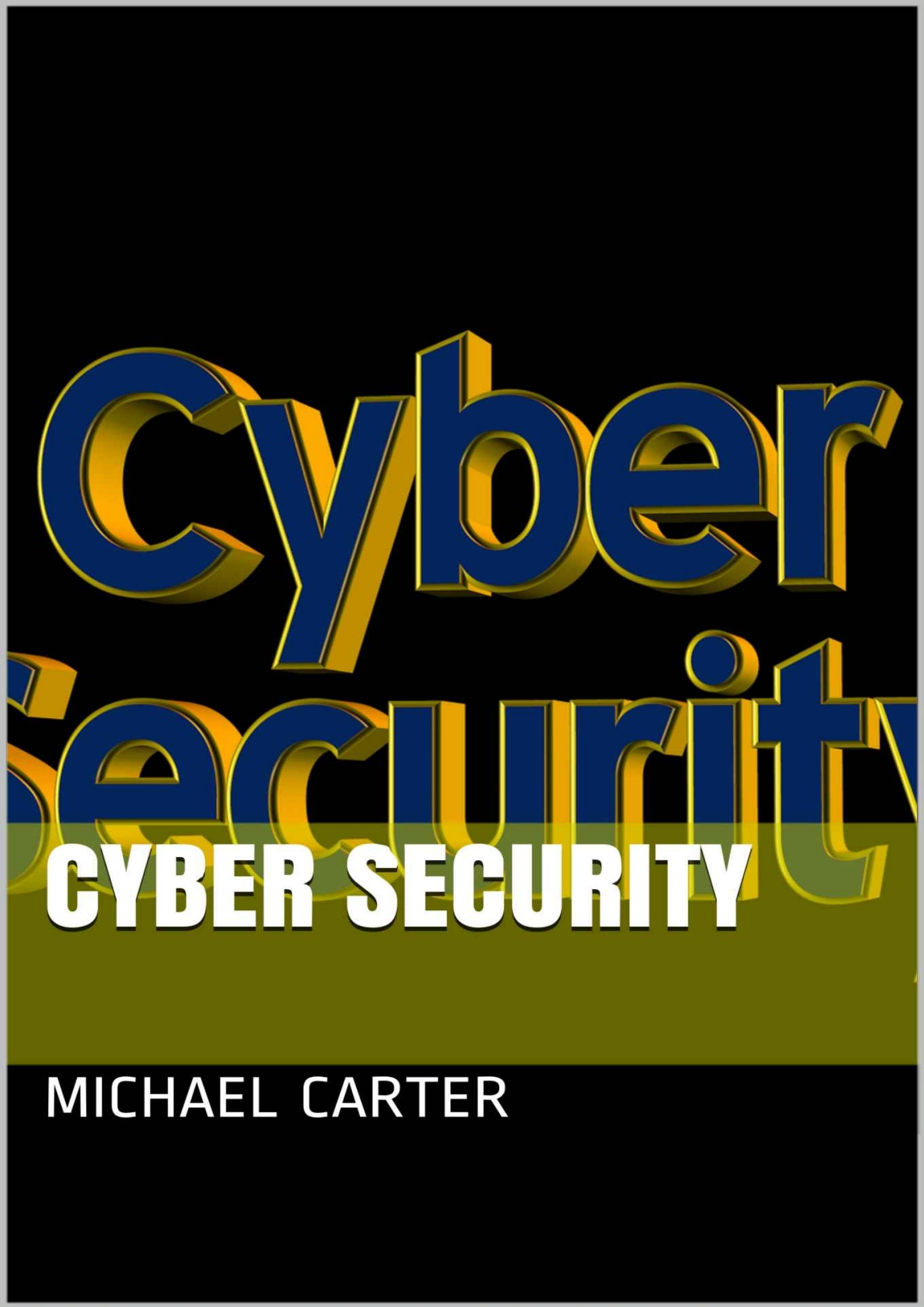

CYBER SECURITY

MICHAEL CARTER

Computer Security

Written by: Michael La’ Del Carter

Computer Security

You awake to the combination of alarm clock buzzer and radio as your alarm clock strikes 6:00am. With reality and the new day, all a tired and sleepy blur, great you with the sun casting forth its warm and gentle glow through your bedroom window you stretch forth your arm from beneath the warm blankets to hit the snooze button.

You climb slowly out of bed. Your first urgent thought of the day rushes to a reminder that you wrote yourself the night before on a note stuck to your refrigerator door the night before and it reads “Important, check email for confirmation import and export meeting scheduled at 2:30pm today with the sales committee at work.” You jump from your bed.

You jump into the shower, brush your teeth, put on your work clothes, and comb your hair. Before you fix breakfast you rush to your computer located in your home office and begin going through your emails. As you scroll through your emails you notice an email from what looks like a reputable real estate company you were recently researching; it is that you’re planning to move to a new school district – next year is Jr. High for your son.

As you open the email you notice that homes are in an area you prefer and they are being offered on the courthouse steps for what they cost in property tax for the year. There is a form. You fill it out. You give your name, age, current address, current employer, number of people in your family, your social security number for a credit check, and your date of birth. You see it all as harmless. Once the form is filled out a message appears that an agent will contact you in a day. Then you return to your confirmation email.

What you did not know based upon mere appearances is that your email from the real estate company was a sophisticated attack by a hacker to gain your most personal information to begin opening bank and credit card accounts in your name, purchase property, and monitor your credit rating as well as take control of your computer system. The design is called malware a malicious URL.

A URL is an electronic address of a Web site that is hosted over the Internet. Malicious URL’s are one of the most popular and illusive means of attack hackers use for just these purposes. The URL’s are usually backed by malicious code. Code is a term used to define commands or programs written in a computer language designed to give a computer explicit instructions on how to behave and carry out computer sequences or processes.

Once you have interacted with the URL or Web site the prompts you are given are designed to be hidden in what these interactions are accomplishing to you – the end user, however, the result is your actual cooperation in your own hack. There are 1 trillion Web sites hosted over the Internet and 1.5 billion cyber-attacks every four months and the odds of you never encountering a malicious URL or malware are extremely low.

Generally these attacks have one or a combination of purposes theft, fraud, copyright infringement, sabotage (the planting of Trojans or viruses or bots), taking control of your computer system, and personal attack (blackmail, to discredit, or exploitation etc.)

Technology is one of the most advanced sciences of our time. It is that technology is becoming ever more commercial from social media to business apps and blogs that are seemingly essential to our daily lives both personal and professional. Whether you're a 5th grader or a senior citizen it is technology – the Industrial Revolution that is becoming a necessity.

Science has come a long way since the home computing of the Commodore 64. Today, technology has the luxury of mobile platforms from smartphones, tablets, laptops, Mac's and PC's technology is shaping us.

If one were to try and judge technology from a marketed perspective one would believe she has the perfect tool placed at her disposal with no hidden dangers. What is seen are features and apps, storage, and security not vulnerabilities?

Besides hacks, one has to worry about the way one handles technology. Author of "*Word of Mouse"* Ostrofsky, (2013) highlights this fact with surprising clarity "

> *A lot of activities that people engage in online can damage their reputation in a heartbeat. Take these examples:*
>
> - *Posting or emailing drunken parties*
> - *Blogging details about a nasty divorce*
> - *Recording rowdy videos on YouTube*
> - *Posting names and photos from gay pride meetings*
> - *Blogging about you companies internal matters*
> - *Tweeting about a disgruntled customer*
> - *Discussing workplace disputes on Facebook*
> - *Seeking public opinion about business issues via email or online forums*

Typically, most people maintain a minimum of 50 friends on Facebook, Twitter,

Instagram, and MySpace. As of the writing of this article the 2016 Presidential elections are the topic of social median and mobile media forums. Political propaganda is being shared, discussed, and evaluated. Emotions are running high and the atmosphere is charged. What is happening is that people are creating a political reputation that will stay on the Internet for the life of it.

The tragedies of suicide and hazing are just a few drawbacks to the social media and mobile media stage and it is the human factor, which we will talk about a little later, of computing that also bears a great deal of weight as to what we fall victim of and how much security we have.

What happens when a vegetable garden becomes a haven for Adders, Scorpions, Africanized Killer Bees, and Jackals? The owner makes war on the invaders ruining her produce! It was the military who developed the Internet and not for a whole slew of purposes it is being used for. The Internet became public with the hopes that its speed, connectivity, and resources would make for better opportunities for business, education, and personal computing. The Internet today is known by the military as the fifth domain of war. The first four are of course land, air, sea, and space.

In 2006, the United States of America suffered a loss of highly classified military design and technical information that could very well shape the outcome of war in the future for the U.S. Who's done this? Where did this take place? What was the purpose? How did it happen?

It was known that it was China. According to the author of the fascinating and enlightening book "*@ war: The Rise of the Military-Internet Complex"* Harris, (2014)

> *For decades China had waged an aggressive campaign of espionage against the U.S. Armed Forces, its most formidable adversary. Beginning in the late 1970's, China with its agents working in or visiting American Universities, government research labs, and defense contractors made off with design information about weapons systems, including nuclear weapons.*

The F-35 was the target. The cost to replace one was at the time a whopping $337 Billion dollars. Instead of hacking into the U.S. networks the Chinese hacked into the defense contractor for the U.S. Lockheed Martin's network who was the hired contractor for the F-35 and stole the designs from their computers.

One thing is for sure this event and others similar to it has constituted that among all that it is doing the Internet is now a battlefield. The National Security Administration

(NSA) has formed groups like the Tailored Access Operations Office (TAO) to conduct its own Internet espionage operations. Working closely together with the Central Intelligence Agency (CIA) is the NSA and its group the TAO. Remember, there are always casualties when it comes to war.

The enemy is among us. The Internet is the battleground where threats against citizens, banks, and power grids are realities. How we utilize technology will become more important as we face threats from terrorist organizations, crime rings, and nations.

In the mind of the average person when he or she might be asked to constitute what calls forth the need for computer security their first thought that comes to mind could very well be attacks. It is that since the new industrial revolution with technology leading, the need to protect information from attacks has had more than its share of time in the headlines. The truth is told the lack of information security is costing 10's of Billions of dollars annually.

Today, the cloud is the latest and most vulnerable of technologies. Attacks happen to one or a combination of vulnerabilities computing systems inevitably possess; the *hardware*, the *software*, or the *data* itself. The cloud possesses all of these vulnerabilities as well.

What the cloud actually is might startle you. The cloud can be accurately described as a farm yard of servers that are hosted by the Internet where software applications can be run for both personal or business; businesses run some of their processes on cloud servers to save costs associated with space and cooling/ventilation, and information is stored in the cloud, for example, customer data and credit card numbers.

The two main vulnerabilities to the cloud are the software running the cloud and the data that is housed there. If the software protecting the data is compromised then the data can be compromised as well. Hackers spend all of their free time learning how to compromise and steal. For them it is a high. The hardware that makes up the cloud is generally the most secure being housed in a physical building that is secured.

As of 2014 the U.S. government is spending $13 Billion dollars annually on cloud services, Pacella, R. M. (2013). It is been stated that cloud computing is the most vulnerable form of technology by nature of the remote accessibility that is the cloud. Not to mention that the layers of software used to run the cloud are becoming ever more vulnerable to malicious code. Malware is malicious code that hackers are using to infiltrate the cloud.

There are literally millions of malicious URL's that are sent across the Internet with only one purpose; to be used as a distribution channel for malware attacks. However, the allure of the speed of Internet computing is, too, compelling and valued to turn away. We can safely assume business will not anytime soon seek new channels of information processing, distributions, and purchasing.

Web applications and services have been developed and deployed at an unprecedented speed, providing various important functionalities to the end-user such as office applications, social networking, content sharing, education, and entertainment. From 2005 – 2008, the number of index able Web pages has grown from a few billion to a trillion. In 2010, the population of Internet users was about two billion. Moreover, the numbers are rapidly increasing, Chang, et al (2013).

So, what is really waiting as far as attacks over the internet; and, how is it again that malware is so dangerous; how will I become an unassuming victim? Malware is the most prominent form of attack over the Internet. All one has to do to become a victim of malware is visit a malicious Web site. Malware will then begin the process of gaining control of your computer system, stealing private and sensitive information, launching denial of service attacks and spamming just to name a few – others launch other malware software into your computer system creating a virus as well as any combination of the other crimes.

What is the best solution to these attacks? Firewalls (in various degrees of sophistication) are the first shield against these types of malware attacks. This is primary effective because of the way these attacks are carried out. "Attackers actively search for and infect victims systems," Chang, et al (2013).

In doing some research for this article on computer security I found a company who is definitely in the fight against cybercrime and especially the threat of malicious URL's. The company's name is ***Proofpoint***. Proofpoint was the winner of the Best Email Security Solution Trust Award by SC Magazine for 2016. Proofpoint provides enterprise level protection where firewalls are being used to combat these threats on PC's, Mac's, Laptops, tablets, and mobile devices.

Did you know that 90 percent of all targeted attacks start with an email, says Kalember, (N.D.) Senior Vice President of Cyber security Strategies for Proofpoint? Proofpoint has stood out and been recognized by SC Magazine for its enterprise protection here's what they offer:

1. Advanced Threat Protection: Effectively block unknown threats and predictively block new, emerging threats and campaigns
2. Threat Classification and Real-Time Analysis: Powerful threat classification and real-time analysis of threats across entire organization
3. Unmatched Control: Rich email policy options enable fine tuning of email routing, handling and quarantine rules
4. Robust Delivery and Administration: Flexible, scalable architecture and administration for appropriate delegation and controls

For personal computing the best way to avoid hacks and attacks add firewall protection and Internet Security in addition to the package that comes with your operating system the top 5 suites are:

1. McAfee
2. Bitdefender
3. Norton
4. BullGaurd
5. Avira

Do not add more than one in addition to your standard Internet security suite or they will think the other is a virus and begin to attack it. There are plenty of free firewalls you can download that add great protection Zone Alarm is just one that I use.

In conclusion, in the mind of the average person when he or she might be asked to constitute what calls forth the need for computer security their first thought that comes to mind could very well be attacks. It is that since the new industrial revolution with technology leading, the need to protect information from attacks has had more than its share of time in the headlines. The truth is told the lack of information security is costing 10's of Billions of dollars annually.

Today, the cloud is the latest and most vulnerable of technologies. Attacks happen to one or a combination of vulnerabilities computing systems inevitably possess; the *hardware*, the *software*, or the *data* itself. The cloud possesses all of these vulnerabilities as well. If you are a business check out ProofPoint and if you're a personal user then get additional protection in the form of Internet Security suites and added firewalls which are free for the downloading if you search "Free firewalls downloads."

Chang, J., Venkatasubramanian, K. K., West, A. G., and Lee, I. 2013. Analyzing and

defending against

Web-based malware. ACM Comput. Surv. 45, 4, Article 49 (August 2013), 35 pages.

DOI: http://dx.doi.org/10.1145/2501654.2501663

Ostrofsky, M. (2013) *Word of Mouse* New York, NY. Simon & Schuster

Harris, S. (2014) *@ War: The Rise of the Military-Internet Complex* Boston, NY Houghton Mifflin Harcourt

Pacella, R. M. (2013). Hacking Is a Significant Threat to Cloud Computing. In D. Haugen & S. Musser (Eds.), *At Issue. Technology and the Cloud.* Detroit: Greenhaven Press. (Reprinted from Popular Science, 2011, April, 278) Retrieved from undefined

Proofpoint (2016) Proofpoint threat report retrieved from https://www.proofpoint.com/sites/default/files/proofpoint_threat_report_-_december_2015.pdf