Brandon Eatmon

IT1025 Final

**Everything about Cyber security**

In modern times society is evolving more in heavy with Technology. Its where we store pretty much everything about ourselves. What our interest are, are shopping habits, financial transactions lead to requiring a bank account or debit card information online. In some ways we are installing all these things about us online. Whether be it Facebook to linked into online address data bases of where we live or have lived. We are slowly becoming apart of technology with ourselves it has become a need even to some degree an essential to have some type of Technology by your specifically the type that accesses the internet. Cell phones and Pcs are a daily need. Its where we can access our money, future money (Stock), store where we been, our deepest secrets, our favorite shows, work documents and the list can go on and is constantly growing every day. With this evolution of society having all of that precious information about protected is a must. If not, someone can destroy your life with just the internet which Is why the most underrated aspect of this evolving society is its cyber security. It it becoming the most important thing we all must have.

The first digital computer was created in 1943. They were extremely large and loud. Most people didn’t have the earliest computers. For most they didn’t even exist to many in society. Furthermore there was no network connection either. Yet John V. Neumann theorized some type of “Mechanical organism” that would damage the machines could be possible. He later wrote about it in a paper in 1966 called Theory in self reproducing automata.

In the 1950s the first use of hacking wasn’t as malicious and devious as today. Back then its goal was hijack protocols engineers had in place to work on the networks from a distance. This made calling free. Companies had no way to defend it and they just had to deal with it for a while.

The term hacking didn’t start until the 1960s. The first hacking came when a group of people hacked the MIT Tech Model Railroad Club hacked high tech train sets. They wanted to adjust their functionality. That same premise made the move to computers this year.

Still, hacking and gaining access to these early computers didn’t seem like “big business.” In fact, these early hacking events simply aimed to gain access to systems. There were no political or commercial benefits likely to occur, though. Rather, early hacking was more about causing some trouble to see if it could be done. In 1967 a student exploited IBM systems vulnerabilities when the company brought a group of students to try their new designed computers. This was extremely key. As IBM had now understood they computer systems vulnerabilities. The effect created a defensive mindset to the game the made sure they had security to keep hackers out.

The true birth of cybersecurity occurred in the 1970s. This began with a project called The Advanced Research Projects Agency Network (ARPANET). This was the connectivity network developed prior to the internet itself. A man named Bob Thomas determined it was possible for a computer program to move over a network. As it did so, the program would leave a trail as it moved. He developed the program so that it could move between the Tenex terminals on ARPANET. Mr. Thomas called this program Creeper. Mr. Thomas created the program to carry and print a simple message. “I’M THE CREEPER: CATCH ME IF YOU CAN.” This sparked a lot of interest and some concern. It was this message that spurred a man named Ray Tomlinson to develop a new program. He called this program Reaper. Tomlinson, who gained fame for his development of email, developed Reaper to chase and delete Creeper.

Reaper is easily the first example of an antivirus software program. It was also called a self replicating program. That made Reaper the world’s first computer worm. During the mid point of this decade it became a focus to work on safe and secure systems. The Electronic Systems Division (ESD) of the U.S. Air Force Command began working on projects. The Advanced Research Projects Agency (ARPA) was also involved. It was a division of the U.S. Defense Department. Their task was to develop security for the Honeywell Multics (HIS level 68) computer system. By 1979 the first cyber criminal had been arrested Kevin Mitnick at just 16 years old. He hacked the ark which was a massive system used for developing operating systems. Just the beginning of nightmarish hacking to come.

During the 1980s famous cyber attacks at AT&T, the Los Alamos National Laboratory, and National CSS happened. 1983 these hacks were deemed terms like “computer virus” and “trojan horse”. These threat become a problem for governments with their potential and the cold war was happening at this time which heightened the level of this threat. Which birthed the orange book a guide for for security of computers this is the first of its kind. It aimed to assess how much trust is put into software that uses any type of sensitive information. It also established some basic security measures that software manufactured need to consider. This would create a foundation from which commercial computer programs were developed in terms of cybersecurity. When Marcus Hess hacked the government he gained access to over 400 military computers and attempted to sell them to the KBG. In 1987 the first antivirus products were developed and released. The Vienna virus was the first form of malware. The cascade virus soon came after the first encrypted virus. Then the computer worm came next. It was a furry of attacks happening and these systems developer had to find ways to stop them as they only became more advanced and bigger as time passed. The response was more effective antiviruses like Norman virus control, ThunderBYTE and F-Prot. IBM also released the first virus scan and MS-DOS solutions.

In the 1990s The Polymorphic virus risks developed. It’s the first code that mutates as it infacts computers and pc. It was made to avoid detection which made it hard to track. Cybercriminal warfare kept growing as they developed the first anti antivirus program. By 1996 the macro virus and stealth capability became a problem. This required more development to made to antivirus software due to the challenges it caused. They keep coming the ILOVEYOU and Melissa virus surfaced which slowed down email system which caused them to fail. This new viruses were looking for financial gain and had planned agendas. Secure Socket Layer and Hypertext Transfer Protocol Secure was soon put in place to help.

In the 2000s Everything continued to grow. Computers were becoming more and more common everywhere. During this time a new type of infection could happen where you didn’t have to download a virus but simply open a web page already infected would be enough. The first hacker groups came about. Hackers these days aimed for credit cards. The Albert Gonzales group was a targeted. With te group of hackers gaining access to 45.7 million credit cards. 3 billion people had their yahoo accounts hacked in 2013 and 2014. New solutions had to be found. Thus, created new detection methods and solutions which included a list of things. Computer forensics, Multi factor authentication, Network Behavioral Analysis, Real time protection, sandboxing, back ups and mirroring and web application firewalls just to name a few.

Cyber threats are still very powerful and more problematic. Just a while ago the gas lines were held hostage for money. Which Colonial Pipeline paid nearly $5 million for it. It put the world in a panic frenzy to buy all the gas they could. System monitoring became more important along with IT governance. The power of a cyber attack can steal all your money and even cripple governments as many have come close. The value of cyber security is an must for society to fully function properly whether that is a good thing or bad thing can be debated. We must continue to create strong and better anti viruses because this warfare over the control of the internet and its access will not stop. It seems like nothing but a blow for blow fight over the power of the internet. Only can hope viruses don’t become deadlier. They likely will continue to get more complex and trickier. We gotta find solutions before they even are thought of by hackers. As impossible as it sounds this blow for blow fight will keep happening the more power the internet gains in society. I think that’s the only way to ensure a hacking becomes extinct.

Source : <https://cyber-security.degree/resources/history-of-cyber-security/>