# The Evolution of Cybersecurity

When ENIAC, the first modern computer, was brought online in 1945,Cyber security wasn't a word you could find in the dictionary. The only way to interact with the building-sized computers of the era was to be physically present, so virtual threats weren't a risk, and access control was a matter of physical security.

Cybersecurity developed as a distinct field throughout the 1960s and 70s and exploded into the public consciousness in the late 1980s, after a series of events that highlighted just how dangerous a lack of security could be. Continuing to grow throughout the 90s, cybersecurity is now a core part of modern life. Let's explore the brief history of this field.

**Origins**

When you hear the word "hacker", you probably think of a mysterious individual sitting alone in a dark room, watching information scroll by on multiple windows as they conduct nefarious deeds.

**The 1960's**

The more connected we are, the more important cybersecurity is, and the widespread adoption of time-sharing in the 60s was a big increase in connectivity. Computers of the era were expensive and bulky; timesharing let multiple people use a single large computer at the same time, which meant that precautions were needed to prevent unauthorized access to files and to the computer itself. Computing time was expensive in those days! The solution of protecting accounts with passwords has persisted to modern times.

**The 1970's**

The creation of ARPANET, the earliest form of the internet, gave hackers a lot to think about and explore. ARPANET was a testing ground for new technologies, and the hacker and technical communities busied themselves with developing and prototyping new technologies, including email. There were a few adventures into the development of malware (short for malicious software), including Creeper and Reaper, the first computer worms, but these were academic exercises more than anything else.

```
I'M THE CREEPER; CATCH ME IF YOU CAN
```

*The message you would have seen if you received a visit from Creeper!*

In this era of rapid development and experimentation, the security of the technology being developed was not a concern. The widespread view of ARPANET as a cooperative academic endeavor and the absence of well-established best practices meant that the motivation and means to design secure systems and software were limited. However, people were starting to think about security. A 1975 paper titled *The Protection of Information in Computer Systems* presented principles and concepts that would become critical to cybersecurity in the future.

**The 1980's**

The 1980s were a chaotic time; the Internet was formed in 1983, and the adoption of the Internet Protocol Suite by ARPANET and other networks added more potential targets and attackers to the mix. The first "real" malware emerged during this time, as did the public panic around The Cold War. Tools and techniques developed during this era would become common in modern cybersecurity; dictionary attacks used stolen lists of passwords and exploited weak default credentials, while decoy computer systems trapped attackers.

The late 80's gave two major events.

- The first was the discovery that a hacker working for the KGB gained access to sensitive documents from the U.S. military.
- The second was the creation of the world's truly serious piece of malware: the Morris Worm. It was originally written to map the size of the internet but quickly grew out of control, choking computers with multiple copies of itself, and clogging the network as it kept replicating.

These incidences exploited unsecured default settings; default passwords like "admin" ensured a system or piece of software was easily exploitable.

**The 1990's**

The 1990s are widely considered to be the era of viruses. Computers that connected to the internet became more common in households and this increased access. This led to unskilled *script kiddies* — individuals who

download a piece of code and run it without having to write any code themselves. They can use that code to launch attacks they don't understand in order to vandalize or destroy targets for fun.

The unfocused, scattered attacks of the era led to the rise of the anti-malware industry, evolving from a curiosity to a core part of modern cybersecurity. Cybersecurity, as a whole, started to be taken much more seriously. Large companies made public pushes to improve the security of their products. Household computers were often targeted by the rampant malware of the era, demonstrating the consequences of poor cybersecurity to their owners.

**The 2000's**

More and more data became digitized — particularly monetary transactions. As the script kiddies of the 90s grew up and gained more experience, the scale of threats shifted, and attackers started having larger targets beyond vandalism and destruction. Credit-card breaches, hacktivism, and holding corporations' systems for ransom became increasingly common, as malicious hackers realized there was real money to be made from cybercrime.

Hundreds of millions of sets of credit card data were breached over the course of the decade.

The threats of data breaches and ransomware attacks forced large businesses to improve their cybersecurity programs. Being hacked was no longer just a matter of vandalism; it could lead to extended downtime, loss of customer loyalty, lawsuits, and fines from regulatory bodies.

The 2010's

During the 2010s, the scale of threats continued to grow: Attacks by nation-states increased in frequency, and they carried out infiltration and surveillance campaigns and deployed cyberweapons to attack strategic objectives. Malicious hacker groups targeted major corporations and government organizations, stealing data and launching ransomware attacks, and the growing number of smart devices in circulation gave these groups an entirely new type of target.

The most dangerous of these new threat actors are known as APTs: Advanced Persistent Threats. Often funded by nation-states, APTs

possess resources and determination far beyond what smaller threat actors might have access to. While lesser threat actors might be capable of launching cyber attacks against a target, APTs are capable of running entire cyber-campaigns, attempting to infiltrate their target across multiple domains simultaneously.

Large-scale cybersecurity incidents became more and more common: WannaCry and NotPetya caused global damage, the [Equifax) and Yahoo! breaches revealed hundreds of millions of pieces of personal information, and countless companies and organizations were hit by ransomware attacks, bringing their operations grinding to a halt.

The present

With the world as connected as it is, cybersecurity is about protecting people as much as it is about protecting computers. People are fallible, and, like computers, we have vulnerabilities that can be exploited: Emotional manipulation and social engineering are powerful tools, used by hackers to gain access to secure systems. Many of the systems we rely on run on computers, and the stakes for protecting them have never been higher. Attacks on those computers can disrupt transportation, power, economy, healthcare, communication, and even lives.

With computers so integrated into our lives, it's crucial that we protect them. In cybersecurity, we must learn from our mistakes, applying the lessons learned in the past to prevent attacks in the future. This is the domain of security researchers and ethical hackers: Finding and fixing vulnerabilities before they can be exploited, and helping to make us and our computers as safe as possible.