The History of Cybersecurity

In today's increasingly digital world, cybercrime continues to be a growing threat. It is an illegal activity that uses the internet or computer networks to commit a crime, such as hacking, identity theft, fraud, intellectual property theft, and cyberstalking. Effective cybersecurity can reduce the risk of cybercrime and protect individuals, organizations, and societies from its negative consequences. The term "cybersecurity" refers to the practices and technologies used to protect computer networks, devices, and sensitive personal information against unwanted access, use, disclosure, disruption, alteration, and destruction.

In this blog, we will provide you an overview of the history of cybersecurity.

The origin of cybersecurity began in the 1960s with the first computer networks. The main concerns were technical issues such as network reliability and data transmission. As computers and networks became more widespread and the valuable data being stored and transmitted increased, the need for security measures to protect against unauthorized access, theft, and data manipulation became more evident.

Actual cybersecurity originated in the 1970s when Robert (Bob) Thomas, a Cambridge researcher for BBN Technologies, discovered the first computer virus (worm) in 1971, known as the "Creeper virus." Ray Tomlinson, the inventor of email, took Thomas's idea and developed the first self-replicating program, Reaper. "Reaper" was the first antivirus program to detect and eliminate Creeper copies.

The emergence of the Internet and advances in computer technology increased the demand for cybersecurity. In 1987, the first firewall was invented, securing computer networks from unauthorized access. In the same year, the Computer Emergency Response Team (CERT) was established to assist organizations with security incidents.

Increased computer viruses and hacking attempts in the late 1980s and early 1990s sparked the development of antivirus software and security technologies. In 1988, the Morris Worm was unleashed, infecting thousands of computers and causing widespread disruption. This incident highlighted the need for more significant security measures and the importance of coordinated response efforts.

During the 1990s and early 2000s, the Internet became more widespread, leading to increased cyber-attacks and the development of new types of malware, such as Worms and Trojans. The 9/11 attacks in 2001 brought the issue of cybersecurity to the forefront of national security concerns, leading to the Department of Homeland Security creation in 2002. It also increased the government's investment in cybersecurity.

Over the past decade, mobile and cloud computing use has skyrocketed, presenting new risks and opportunities for cybercriminals. The rise of Big data and the IoTs has further increased the amount of valuable data stored and transmitted, leading to an increase in cyber-attacks and data breaches. Today, cybersecurity is a critical concern for individuals, businesses, and governments.

How can InfosecTrain help you?

As the world becomes increasingly interconnected, the importance of cybersecurity will continue to grow, and the field will continue to evolve in response to new threats and technological advancements.
InfosecTrain is a well-known online training and certification provider for cybersecurity, information security, and cloud security domains. If you aspire to start your career in the field of cybersecurity and become a Cybersecurity Professional, check out our courses and enroll for the most suitable course to advance your career.