Women in Tech

A Beginner's Guide to the Cyber World

# STEPPING INTO CYBERSECURITY

## WHAT DOES CYBERSECURITY USUALLY MEAN?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

## THERE ARE ROUGHLY SIX DIFFERENT FIELDS IN CYBERSECURITY.

The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

## NETWORK. APPLICATION. INFORMATION.

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
Application security focuses on keeping software and devices free of threats.
Information security protects the integrityand privacy of data, both in storage and in transit.

## OPERATIONAL. DISASTER RECOVERY. END USER.

Operational security includes the processes and decisions for handling and protecting data assets. Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. End-user education addresses the most unpredictable cyber-security factor: people.

# THE SCALE OF THE CYBER THREAT

## TYPES OF CYBER THREATS ENCOUNTERED ARE THREE FOLD.

## CYBER CRIME. CYBER ATTACK. CYBER TERRORISM.

Malware means Malicious Software and it is the most common cyber threat. It can damage or disrupt a legitimate user's system in forms of Virus, Trojans, Spyware, Ransomware, Adware, Botnets, SQL Injection, Phishing, Man-in-the-middle Attack or Denial-of-service attack.

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

## LATEST CYBER THREATS

-Dridex malware
In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack.
-Romance Scams
In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps.
-Emotnet Malware
Emotet is a sophisticated trojan that can steal data and also load other malware.

## END USER PROTECTION

End-user protection or endpoint security is a crucial aspect of cyber security.
After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.
So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data.
This not only protects information in transit, but also guards against loss or theft.

## Protect Yourself Against Cyber Attacks.

*The best you can do is updating your software and OS as that means your are benefitting from the security patches.*