THE CYBER THREAT IS REAL

**TYPES OF ATTACKS**

- **VIRUSES & WORMS**
  Code that infects computers through security failures and replicates itself to spread to other computers.

- **CYBER ESPIONAGE**
  A stealth attack to gain access to a network and exfiltrate sensitive information and data.

- **MALWARE**
  Malicious software is code designed to damage, disrupt, infect or control networks, controllers, computers, or data.

- **ACCESS-BASED ATTACKS**
  Exploiting compromised digital certificates and passwords to access networks. In 2012, the software to steal certificates increased 10x.

- **HACKING ATTACKS**
  Hackers can infiltrate networks and computers, and compromise sensitive information more easily as data becomes more interconnected.

**LEAD**
The Navy Cybersecurity Division leads by ensuring a comprehensive approach to cybersecurity is taken across all Navy missions.

**ACQUIRE**
Focus is on strengthening cybersecurity throughout the product lifecycle. SPAWAR is the Navy’s Technical Authority for cyber and provides the architecture and technical standards required to harden the Navy’s networks and equipment.

**EQUIP**
Information Dominance Forces Command (NAVIFOR) organizes, mans, trains, and equips the cybersecurity workforce.

**FIGHT**
U.S. Fleet Cyber Command /50th Fleet commands a full spectrum of cyber warfare capabilities across all warfighting domains.

**NAVY CYBERSECURITY TEAM**

- The annual global cost of cybercrime against consumers is 113 billion dollars.
- The DOD experiences 41 million scans, probes and attacks per month.
- Intrusions into critical U.S. infrastructure have increased by 17 times over the past three years.
- The average cost of resolving a single cyber attack is now 1.6 million dollars.
- Cybercrimes now take approximately 33 percent longer to resolve than 5 years ago.

**ATTACK STATISTICS**
Cyber attacks have monetary and mission impacts.

**CYBER ATTACKS EVOLVE**

- **“Morris Worm” attack**
  Infected 60,000 computers, caused $100 million in damage (1988)

- **“MafiBoyz” attack**
  A 15-year-old boy attacked commercial websites, causing $1.2 billion in damage (2005)

- **TXJ hack**
  Hackers gathered credit card data on more than 94 million T.J. Maxx consumers (2005)

- **OPM data breach**
  Hackers potentially stole information on more than 21.5 million current and former federal employees (2015)

Sources:
- OPNAV N2/N6
- Harvard Business Review