The 5 Most Researched Cyber Security Topics and Why They Matter

Cyber security is a vital field of study and research as cyber-attacks pose serious threats to individuals, businesses, governments, and society. By examining the most researched cyber security topics, we gain a better understanding of the breadth and complexity of the field and issues business leaders need to address.

The Costliest Cyber-Attacks

According to online sources, the two most costly cyber-attacks of 2023 in the United States involved the hacking of US satellite communications provider, ViaSat, by Russian state-sponsored actors, and the massive ransomware attack on contractors of the U.S. Department of Health and Human Services (HHS).

- The ViaSat attack disrupted the GPS and communications systems of several U.S. government agencies and critical infrastructure sectors. It caused an estimated $1.2 billion in damages.
- The HHS attack encrypted the data of more than 100 million patients and demanded $500 million in Bitcoin for the decryption key. The attack also exposed sensitive personal and medical information, leading to lawsuits and identity theft.

Both attacks highlight the vulnerabilities of the U.S. digital ecosystem and the need for more robust cyber security measures and resilience strategies. Fortunately, cyber security research contributes greatly to the protection and advancement of digital society.

The Most Researched Cyber Security Topics

Cyber security researchers study the threats and vulnerabilities that affect various systems and networks, such as computers, smartphones, cloud services, and critical infrastructures. They develop methods and tools to prevent, detect, and mitigate cyberattacks. Their work serves to enhance the resilience and trustworthiness of these systems and networks.

Cyber security research also informs policy makers, industry leaders, and the public about current and emerging challenges and opportunities in cyberspace. Below, we explore five of the most researched cyber security topics and why they are important for the present health and future utility of cyberspace.

Data Privacy

Data privacy refers to the right of individuals to control how their personal information is collected, used, shared, and stored online. Data privacy laws seek to protect an individual's identity, reputation, preferences, and sensitive information from hackers, advertisers, or malicious actors.

Data privacy research focuses on developing encryption techniques, privacy policies, consent mechanisms, and anonymization methods to safeguard personal data.

AI and IoT Security

Artificial intelligence (AI) and the Internet of Things (IoT) are often found in the headlines. They have the potential to transform our lives in the areas of health care, education, transportation, and entertainment. However, they also introduce new security challenges, such as malicious manipulation, unauthorized access, data leakage, or cyber-attacks.

AI and IoT security research efforts aim to ensure the safety, reliability, and trustworthiness of these technologies and their applications.

Quantum Technology and Space Communication

Quantum technology exploits the properties of quantum mechanics, such as superposition and entanglement, to perform tasks that are impossible or impractical with classical computing methods. Quantum technology seeks applications in computing, cryptography, communication, sensing, and metrology.

Space communication is the transmission of information between spacecraft or between spacecraft and Earth. Both quantum technology and space communication require advanced levels of security to prevent eavesdropping, interception, or tampering.

Quantum technology and space communication research explores how to achieve secure quantum and space communications using quantum key distribution (QKD), quantum cryptography, quantum error correction, or quantum repeaters.

Cyberethics, Criminology, and Law

Cyberethics includes the study of the moral and ethical issues related to cyberspace. Relevant cyberethics issues include privacy, intellectual property, freedom of expression, cyberbullying, or digital citizenship.

Criminology encompasses the study of the causes, consequences, prevention, and control of crime in cyberspace. Topics studied include hacking, phishing, fraud, identity theft, cyberterrorism, or cyberwarfare. Cyber security law examines the legal frameworks and regulations that govern cyberspace at national and international levels.

Research in the areas of cyberethics, criminology, and cyber security law analyzes how to balance the rights and responsibilities of cyber users and stakeholders while ensuring justice, accountability, and physical security as well as security in cyberspace.

Malware

Malware includes any software designed to harm or disrupt a computer system or network. It can take various forms, such as viruses, worms, trojans, ransomware, spyware, or adware. Malware causes a wide variety of damages, such as deleting or encrypting data, stealing information, spying on users, hijacking resources, damaging reputation, or compromising security.

Malware research investigates how malware works, the criminals behind malware, how to detect, analyze, and remove malware, and how to prevent malware infections.

Leverage the Most Researched Cyber Security Topics and Experts

Cyber security is a dynamic and interdisciplinary field that requires constant collaboration and innovation to address the evolving threats and challenges in the digital world.

The cyber security experts at eMazzanti Technologies employ continuous training, new technologies, and advanced certifications to stay ahead of the threats. Business leaders leverage their expertise to assess cyber security risks and protect customer data and valuable business assets.