I'm not a bot

Cyber security ppt

Cyber security is an essential aspect of safeguarding our online presence from potential threats. The term encompasses a range of techniques designed to shield computers, networks, and data from unauthorized access or manipulation by malicious entities. At its core, cyber security involves implementing robust standards that enable organizations to effectively mitigate the risk of successful attacks. This includes protecting communication channels, network infrastructure, and sensitive information against various forms of cybercrime. Cybercrime is a broad term that has evolved over time to incorporate the misuse of digital technology for illicit purposes. The increasing reliance on internet-based platforms has given rise to novel forms of cybercrime, such as hacking, identity theft, and online fraud. Throughout history, cybercrimes have become more sophisticated, with the first recorded incident dating back to 1820. However, it was not until the advent of the internet that these crimes gained widespread recognition. Today, cybercrimes encompass a range of malicious activities, including data interference, system tampering, and misuse of devices. The importance of cyber security cannot be overstated, as it directly impacts our personal and professional lives. To ensure safety online, it is crucial to adopt best practices such as regularly updating software, using strong passwords, and being cautious when sharing sensitive information. Moreover, implementing measures like encryption, disabling remote connectivity, and utilizing reputable antivirus software can significantly enhance cyber security. By remaining vigilant and informed about the latest threats and mitigation strategies, we can better protect ourselves from falling victim to cybercrimes. Ultimately, a comprehensive understanding of cyber security is essential for safeguarding our online presence in today's digital landscape. Cyber threats are constantly evolving, so it's crucial to stay vigilant and keep your digital information safe. Cyber security is a complex field that demands ongoing education to stay ahead of the latest dangers. 1. Staying Safe in the Digital World 2. What is Cyber Security? • Cyber security encompasses various technologies, processes, and best practices designed to safeguard networks, devices, data, and programs from unauthorized access or damage. • Understanding potential threats such as viruses and malware is essential for effective cyber security. • Implementing robust cyber security measures significantly reduces the risk of cyber attacks, protecting both individuals and organizations. 3. Why Cyber Security Matters • The sheer volume of sensitive information stored on computers and other devices by government, corporate, and medical institutions highlights the importance of cyber security. • Protecting this data from major cyber threats is at the core of good cyber security practice. • Some common cyber dangers include: + Cyberterrorism: using IT to disrupt critical infrastructure + Cyberwarfare: nation-states using IT for malicious purposes + Cyberspionage: secretly obtaining sensitive information 4. Common Cyber Threats Explained • Cyberterrorism involves terrorist groups using IT to further their agenda, often targeting networks and communication systems. • Cyberwarfare sees nation-states using IT to penetrate another country's networks and cause damage or disruption. • Cyberspionage is the practice of secretly obtaining sensitive information without permission. 5. Types of Cyber Security Measures • Critical infrastructure security: safeguarding essential systems like power grids, water treatment plants, and hospitals from cyber threats. • Network security: protecting against unauthorized access and malicious insiders. • Cloud security: ensuring data safety in cloud storage solutions, which may not always be secure on their own. • Application security: mitigating vulnerabilities in web applications to prevent attacks. • Internet of things (IoT) security: safeguarding connected devices from cyber threats. 6. Understanding Cyber Security Risks • Critical infrastructure is particularly vulnerable due to its connection to the internet and reliance on interconnected systems. • Network security often requires balancing access control with productivity considerations, such as speed and efficiency. • Cloud providers are developing new tools to help users secure their data in cloud environments. • Application security remains a weak point in many organizations, making it crucial for secure coding practices and regular vulnerability testing. 7. Building Cyber Security Knowledge To stay ahead of the ever-changing cyber threat landscape, download our comprehensive PowerPoint templates on cyber security. Our resources offer a wealth of information to help you build your knowledge and keep your digital world safe. Fuzzing and penetration testing are essential in today's digital landscape. The Internet of things (IoT) security poses unique challenges, with devices often shipping insecurely and offering little to no security patching. This can lead to threats not only to users but also to others on the internet, as these devices may be part of a botnet. Cyber attacks come in various forms, including theft of personal information, corruption or destruction of data, and disruption of services. The attack cycle typically involves six phases: reconnaissance, initial compromise, command and control, lateral movement, target attainment, and exfiltration. To prevent cyber attacks, it is crucial to implement security measures such as two-factor authentication, using unique passwords for each service, and applying software updates regularly. Additionally, avoiding the transmission of sensitive data via email can help minimize the risk of interception by hackers. Furthermore, organizations should focus on fuzzing and penetration testing to identify vulnerabilities in their systems and networks. This involves simulating real-world attacks to test the strength of security measures and prevent potential breaches. Important accounts should not be accessed from public computers, unless absolutely necessary, such as when using a library or coffee shop computer. This includes laptops and desktops issued by the company. Ensure that all devices are covered under Acceptable Use agreements, which should be regularly updated and distributed to employees. The past year has seen unprecedented cyber breaches, with notable incidents like Equifax's massive data compromise affecting nearly half of the country. Hacks have highlighted the vulnerability of personal information. In 2017, a staggering 1.9 billion data records were either lost or stolen due to 918 cyber attacks, most using ransomware that locks files in exchange for payment. Some notable hacks include WannaCry, which spread rapidly in May 2017, and NotPetya, which targeted facilities in Ukraine in July 2017. Additionally, Equifax was breached in September 2017, compromising information of 143 million customers. The Ethereum app platform was also hacked in July, resulting in the theft of $7.4 million worth of Ether. Yahoo's email system was hacked back in 2013 but revealed to be severe in October 2017, affecting 3 billion email addresses and exposing sensitive information that could be used for further breaches. In light of these incidents, cybersecurity predictions for 2018 include the rise of targeted ransomware attacks, including health-related ones, which may even put lives at risk by demanding payment to save a person's life. Given article text here Targeted predictions from Trend Micro indicate that attackers will launch digital extortion campaigns utilizing ransomware to intimidate non-compliant companies under the GDPR regulation. This development aligns with the vendor's expectation of increased emphasis on GDPR compliance. The cybersecurity industry has anticipated this trend due to the looming May 25, 2018, deadline for implementation. AI and machine learning have been often misconstrued as interchangeable terms but are distinct technologies. FireEye predicts a rise in automation, machine learning, and AI adoption to counter cyber-attacks largely due to personnel scarcity. Furthermore, biometric technology's integration into mobile devices, such as fingerprint and facial recognition authentication, has sparked debate regarding its broader adoption in enterprises. Cyber extortion continues to grow, with attackers relying on ransomware and other methods for financial gain. Experts argue that the combination of widespread device usage and anonymous payment mechanisms has enabled large-scale cyber extortion operations. Ultimately, cybersecurity is a strategic business priority rather than an afterthought. Ensuring adequate measures in place can significantly impact a company's standing within its organization. Cyber Security PowerPoint Templates for Effective Communication They offer IT professionals a way to clearly present complex cyber security information to students, teachers, employees, or even clients. Cyber Security Presentation Templates can be used for various purposes such as awareness campaigns, training programs, corporate meetings, product demonstrations, educational lectures, and research presentations. Cyber security is all about safeguarding digital info via online channels, ensuring confidentiality. The concept delves into the measures that safeguard digital assets against cyber threats, followed by an overview of upcoming AI-boosted enhancements for title and description downloads in PPTX, PDF, or TXT formats.

Cyber security ppt class 9. Cyber security ppt free download. Cyber security ppt slideshare. Cyber security ppt pdf. Cyber security ppt presentation pdf. Cyber security ppt in hindi. Cyber security ppt template. Cyber security ppt images. Cyber security ppt free. Cyber security ppt background. Cyber security pptx. Cyber security ppt template free download. Cyber security ppt for school students. Cyber security ppt topics. Cyber security ppt background images.