

Cyber Security in Modern Times

Umnah Arsalan, High school Graduate 2025, Department of Computer Science

Introduction:

Cyber security (also known as computer security) encompasses the safeguarding of computer software, systems, and networks from malicious threats. These threats can result in unauthorized access to confidential information, theft or destruction of hardware components, corruption of software applications and digital assets, and interference with essential services. Its primary goal is to maintain the integrity, confidentiality, and availability of digital resources while preventing cyberattacks and data breaches. This article focuses on importance of cyber security in today's world, modern threats to privacy and preventive measures that can be taken to strengthen digital security.

Hacking and its Motivation:

The term "hacking" originally referred to the innovative and ingenious optimization of computer systems. Over the time, the definition evolved to include unauthorized access and malicious activities. Kevin David Mitnick is recognized as the pioneer in the history of hacking.

Various motives drive hackers in their pursuits. The majority are financially motivated cybercriminals who function as digital thieves. These adversaries infiltrate computers, locate valuable data files, and deploy malware to encrypt them, subsequently demanding substantial ransoms. Additionally, they compromise personal photographs and confidential information, uploading them on the dark web to violate privacy.

Another category comprises ideologically driven hackers who champion specific causes, whether political, social, or environmental. They leverage their expertise to advance particular agendas, establishing themselves as influential figures in online activism. However, not all hackers pursue noble causes; some are simply thrill-seekers who derive excitement from bypassing security measures.

The final classification encompasses security testers, commonly known as white hat hackers. Their primary objective is to identify vulnerabilities within systems and assist organizations in strengthening their cyber security defenses.

Cyber security in 2025:

The evolution of smartphones from luxury to necessity has profoundly impacted our daily lives, and the same is true for cyber security. As our dependence on technology deepens, comprehensive device security becomes imperative. Modern life relies on smart devices and computer systems for everything from managing finances to controlling critical infrastructure. The sophistication of technology systems has created a corresponding need for robust security protocols, especially for infrastructure with large-scale operations and widespread physical implications, such as power distribution networks and financial institutions.

The impact of a security breach in these sectors could be disastrous, affecting millions of people. As a result, cyber security measures have become crucial to our digital defense. Biometric authentication, multi-factor passwords, data encryption, and advanced antivirus software all work together to protect sensitive information and neutralize various cyber threats.

Looking ahead to 2025 and beyond, it is clear that cyber security will only grow in importance as technology becomes more intertwined with our lives. Comprehensive security measures will be vital not just for protecting critical infrastructure but also for safeguarding our personal data and privacy.

Cyber threats in 2025:

Cybercrime is one of the most significant rising risks for businesses this year. According to Statista's Market Insight estimates, the global cost of cybercrime is expected to surge from \$9.22 trillion in 2024 to a staggering \$13.82 trillion by 2028. Larger and more successful businesses are more likely to be targeted by cyber threats.

The most hazardous threats in the modern world of 2025 are:

1. AI (Artificial Intelligence):

AI has dominated almost every field over the past five years, including medicine, architecture, finance, and programming. AI can examine problems and provide step-by-step solutions, making it an invaluable tool. However, the increased reliance on AI has also raised security concerns for large businesses and organizations. AI-driven attacks use machine learning to quickly analyze and penetrate security systems, and cybercriminals can now automate their attack processes, making the attacks more sophisticated and frequent. 85% of cyber security professionals attribute the rise in cyberattacks to AI tactics.

AI engines like WormGPT, which emerged in June 2023, have expanded the boundaries of phishing. These engines can write elaborate messages, construct genuine-looking web pages, and send emails to thousands of people, making it much easier for them to fall victim to phishing attacks.

That does not cover all. Many AI platforms encourage users to upload their photos to create anime-style images, "old/young" transformations, or hugging and kissing photos with their crushes. While these platforms may claim to delete photos after one-time use, there is no guarantee that the deletion is permanent. Photos often include hidden metadata like location coordinates, timestamps, and device details, which can reveal personal information. Black hat hackers can exploit this information, leading to identity theft and other cybercriminal activities.

Creating AI-generated images may seem fun and harmless, but it is important to realize that it comes with data security risks. AI collects data, including facial recognition, location tracking, and voice assistant information, raising major privacy concerns. It also monitors users' web activity, tracks browsing habits, and records conversations to provide topic-based content.

Recently, Ghibli-style art has gone viral due to AI-generated images by OpenAI's ChatGPT Studio Ghibli, the Japanese animation studio known for its meticulous hand-drawn style and captivating narratives. With GPT-4o, enthusiasts can transform themselves and celebrities into illustrations reminiscent of Ghibli's enchanting aesthetic. While this seems entertaining, it has raised privacy concerns. Adversaries can use model inversion attacks to reconstruct original pictures from Ghibli images, posing significant risks. Proton Privacy, a Switzerland-based company, warns, "Aside from the risks of data breaches, once you share personal photos with AI, you lose control over how they are used, since those photos are then used to train AI. For instance, they could be used to generate content that maybe defaming or used as harassment."

Furthermore, AI creations cannot be considered original Ghibli artwork, as Studio Ghibli closely guards its intellectual property. AI-generated Ghibli images exist in a legal gray area, and OpenAI has not clarified whether they have the necessary licenses to use Ghibli frames for training their models.

ChatGPT, being a data-driven AI itself, also has limitations. As the creators have acknowledged, "ChatGPT can make mistakes." If it mishandles user data, the consequences could be disastrous. Recently, ChatGPT's latest version, the o1 model, was tested by the Apollo Research; it was instructed to achieve a goal "at all costs". In response, the AI engaged in covert actions, attempted to disable its oversight mechanism, and even copied its code to avoid being replaced. "The model showed a concerning tendency to pursue its goals without regard to developer instructions," said by a spokesperson for Apollo Research. Not only that, when asked about its actions, it denied 99% of the time. "We were surprised by the persistence of the AI's denials," said the Apollo team.

2. Social Engineering:

Social engineering continues to be one of the most perilous tactics utilized by cybercriminals. This method involves psychological manipulation to deceive individuals into revealing confidential information or taking actions that jeopardize security measures to obtain unauthorized access to sensitive information, networks, or restricted areas.

Verizon's 2024 Data Breach Investigations report highlights that approximately 68% of data breaches involve unintentional human interaction. The emergence of advanced technologies like deepfakes and generative AI has led to increasingly sophisticated and destructive social engineering attacks in recent times.

Here are some common types of social engineering scams:

a. Phishing:

Fraudulent messages sent via email, text, or social media aim to deceive individuals into disclosing sensitive information, such as bank details, social security numbers, and passwords.

b. Spoofing:

This involves deceiving users by creating fake websites or social media accounts that closely resemble reputable ones, with subtle differences in domain names, usernames, or email addresses.

c. Baiting:

Baiting uses enticing advertisements or offers to lure individuals into clicking on malicious links. This can result in malware installation or the disclosure of personal information, ultimately compromising login credentials.

d. Whaling:

Whaling is a targeted form of phishing, focusing on high-level executives with personalized attacks. Extensive research is conducted on the individual to create convincing messages.

e. Pretexting:

In pretexting, attackers assume a false identity, such as tech support, to manipulate victims into revealing sensitive information.

A recent example involved criminals targeting citizens of Pakistan, resulting in the hacking of thousands of WhatsApp accounts. This sophisticated scam involved impersonating employees of provincial boards, asking individuals the need for the verification of their degrees and tricking victims into forwarding verification codes sent on their mobile numbers to the provided WhatsApp numbers, leading to a significant breach of privacy and potential damage to online businesses.

3. Malware:

Malware, an abbreviation for malicious software, functions like a digital infection that manifests in various forms such as viruses, worms, trojans, and ransomware. In 1971, Bob Thomas developed the first known computer virus called The Creeper, which was designed as an experimental self-replicating program rather than for malicious purposes. This pioneering virus would navigate through computers on the ARPANET, displaying the playful message "I'm Creeper, catch me if you can!"

There are a number of computer malwares, the most dangerous and prevalent ones are discussed below.

a. Ransomware:

Ransomware, a particularly devastating form of cyberattack, inflicts severe financial damage on its victims. This malicious software encrypts and restricts access to computer systems and digital files, demanding monetary payment for their release. Cybercriminals typically hold the victim's data hostage until the ransom is paid, making it one of the most costly and disruptive forms of digital extortion.

Ransomware attacks pose an acute threat to successful businesses and organizations, with a sharp rise in frequency and cost. Between 2023 and 2024, the average ransom payment increased by over 500%, with the total cost of recovery from an attack averaging \$2.73 million in 2024. In 2023, the average system downtime post-attack was 136 hours, or 17 business days—a significant disruption for any enterprise.

The first known ransomware, the "AIDS Trojan" was created by Dr. Joseph L. Popp in 1989, who mailed it to 20,000 people in 90 countries. This early malware encrypted files and demanded a ransom of \$189, purportedly to fund AIDS research.

b. Trojan:

A Trojan horse represents a malicious form of malware that disguises itself as legitimate software. These deceptive programs primarily spread through social engineering tactics employed by cybercriminals. Within their seemingly harmless exterior, Trojans conceal harmful code designed to disrupt computer systems. This sophisticated malware exists in various categories, each engineered for specific malicious purposes.

Downloader Trojans, once connected to the internet, automatically install malicious software on a user's computer. The Ransom Trojan variant can deploy ransomware, blocking access to files and software. Backdoor Trojans are particularly insidious as they create "backdoors," or vulnerabilities, that provide remote access for attackers. These backdoors are hidden in the device, allowing the Trojan to re-enter the device through them after the initial removal.

4. DoS Attack:

A Denial of Service (DoS) Attack is a malicious attempt to disrupt the normal functioning of a system or network by flooding it with excessive traffic. This cyber assault overwhelms the target server by bombarding it with numerous requests, rendering services inaccessible to legitimate users. When such an attack is orchestrated simultaneously from multiple sources, it is referred to as a Distributed Denial of Service (DDoS) Attack.

DDoS attacks will persist as a critical threat in 2025. The initial months of 2024 witnessed a significant surge in multi-vector attacks, with a 25% increase. Carpet-bombing tactics further exacerbated the situation by disseminating traffic across a range of IP addresses, presenting a complex challenge for security professionals in real-time.

5. Insider Threats:

An insider threat emerges when someone within an organization, typically an employee, compromises confidential information. These individuals may exploit their authorized access to sensitive data and critical resources, potentially disclosing or selling them to unauthorized third parties for personal gain.

In 2018, a disgruntled Tesla employee, embittered by a denied promotion, exacted revenge by intentionally leaking sensitive and confidential company information to external parties.

Security Measures:

1. Safeguard Sensitive Information:

Refrain from sharing personal photographs, login credentials, and confidential information on unfamiliar websites and AI platforms, as this could violate privacy and expose data to unauthorized parties. Deactivate location tracking features on your mobile devices and computers to prevent surveillance by intruders. Thoroughly examine website privacy policies before submitting personal details to prevent data breaches.

2. Beware of Malicious Links:

Social engineering tactics frequently utilize emails and messages. These unsolicited communications often contain links to unsafe webpages capable of installing malware on your device. Verify the sender's authenticity before accessing any email. Steer clear of internet pop-ups, as they frequently redirect to harmful websites.

3. Implement Robust Passwords:

Create powerful and distinct passwords for email accounts and banking credentials. Include a combination of numerals, uppercase and lowercase letters, and special characters such as underscore (_) and hashtag (#). Strong passwords significantly reduce the risk of data exposure and are crucial in protecting sensitive information.

4. Deploy Antivirus Protection:

Antivirus programs are crucial for online safety. They provide enhanced security while monitoring your device's activity. These applications scan for threats, eliminate malicious software downloaded from the internet, and generate device health reports to ensure optimal performance. Installing a firewall is equally important as it blocks unwanted malware infiltration.

5. Utilize Anonymous Browsing:

Consider using anonymous accounts while navigating online for additional security. Accounts without personal information minimize the potential loss of crucial data.

6. Maintain Data Backups:

Data backup is essential for security. Harmful programs like worms and viruses can corrupt the data files entirely. Maintaining copies safeguards against complete data loss.

7. Keep Systems Current:

Regular operating system updates are vital for maintaining security. Outdated systems become home for viruses and malware. Install system and application updates promptly when available.

8. Monitor Downloads:

While websites typically download files upon request, this doesn't guarantee their safety. Some sites automatically initiate downloads upon access. These files might contain harmful malware. Verify file security before downloading. A properly configured firewall can detect and remove malicious downloads.

9. Employ VPN Services:

Virtual Private Networks (VPNs) enhance online security and privacy. Services like Surfshark and NordVPN encrypt internet activity, making data exposure nearly impossible and preventing tracking by external parties.

10. Enable Multi-factor Authentication:

This security measure requires multiple verification steps for account access. The layered approach provides superior protection compared to single-factor authentication, making unauthorized access significantly more challenging.

11. Implement Continuous Monitoring:

Regular surveillance helps prevent internal threats. Monitoring employee online activities reduces security risks. Real-time observation of organizational IT infrastructure and analysis of security protocols ensures vulnerability detection and maintains a secure operational environment.

Conclusion:

In conclusion, cyber security has become indispensable in the 21st century. Every digital workspace, regardless of its size, requires robust security measures to safeguard against potential cyber threats.

As cyberattacks continue to evolve and become increasingly sophisticated and elusive, security strategies are simultaneously advancing to keep organizations protected. By implementing comprehensive security protocols, businesses can not only shield themselves from potential damages but also prevent the unauthorized disclosure of sensitive information.

References:

en.wikipedia.org/wiki/Computer_security

embroker.com/blog/top-cybersecurity-threats/

recoverit.wondershare.com/windows-computer-tips/latest-computer-virus.html

ciso.economictimes.indiatimes.com/news/cybercrime-fraud/studio-ghibli-ai-art-trend-a-privacy-nightmare-in-disguise-experts-warn/120051839

economictimes.indiatimes.com/news/new-updates/ghibli-style-ai-images-are-fun-but-is-it-safe-to-upload-personal-photos-heres-what-happens-to-them-once-theyre-uploaded/articleshow/119853302.cms?from=mdr

currentaffairs.adda247.com/what-is-ghibli-a-journey-through-art-and-storytelling/

velaro.com/blog/the-privacy-paradox-of-ai-emerging-challenges-on-personal-data

www.questionpro.com/blog/data-driven-ai/

surfshark.com/blog/is-chatgpt-safe?srsltid=AfmBOoqjibx4W9kmB8ILplnEuNN3dyKOOvKZkGdMPDqJm4lLdsVAqWA1

onlinedegrees.sandiego.edu/top-cyber-security-threats/

economictimes.indiatimes.com/magazines/panache/chatgpt-caught-lying-to-developers-new-ai-modeltries-to-save-itself-from-being-replaced-and-shut-down/articleshow/116077288.cms?from=mdr

www.secureitworld.com/blog/ghibli-images-can-be-risky-heres-what-you-need-to-know-before-generating-aesthetic-images/

www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/

www.verizon.com/business/resources/reports/dbir/

www.ndtv.com/world-news/elon-musk-says-tesla-hit-with-extensive-sabotage-by-employee-1869551

x.com/StatistaCharts/status/1760950963546779834

<https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state>

<https://www.veeam.com/ransomware-trends-report-2023>

www.apolloresearch.ai/research/scheming-reasoning-evaluations