11th TNG Youth Leadership Programme 2023 - 2024

CYBERSECURITY HANDBOOK

BY 7A AY-2023-24

INTRODUCTION

WELCOME TO OUR CYBERSECURITY HANDBOOK!

Assalam Alikum, Hello and welcome! We're thrilled to share this journey into the world of cybersecurity with you. In today's digital age, understanding how to protect ourselves and our information online has never been more important. Whether you're browsing the web, chatting with friends, or studying online, cybersecurity touches every part of our digital lives.

MADE BY:

Class Teacher: Ms. Sarah Joy
Mentors: Areeba Naeem (2291) & Ammara Usman (4670)
Students:
Maryam Khan (2168)
Nabiha Furqan (3667)
Zaina Muhammad (3411)
Syeda Hafsa (4059)
Aaisha Atif (1122)
Faha Hareem (1494)
Hibba Afridi (2003)
Umme Kulsoom Umer (3249)

ABOUT OUR TOPIC & THIS HANDBOOK

Our YLP topic this year is Cyber in which we mainly have two sub-topics which are Cybersecurity and Cyberbullying.

This Handbook is a comprehensive guide designed to equip youth with essential knowledge and skills to navigate the digital world safely and responsibly. Through informative content, this booklet covers key topics such as cybersecurity basics, protecting personal information online, recognizing cyber threats, digital citizenship and promoting digital citizenship. By empowering youth with the tools and awareness to make informed decisions online, this handbook aims to cultivate responsible digital citizens and future leaders who can positively impact their communities in the digital age.

WHY WE CHOSE THIS TOPIC?

We chose the topic of cybersecurity for our Youth Leadership Program because it is essential for young people in today's digital world as the Digital world is full of dangers and we want to help spread awareness. Understanding cybersecurity helps students stay safe online, protect their personal information, and avoid cyber threats like scams and cyberbullying. By learning about cybersecurity, students can become leaders in their communities by promoting safe online practices and making a positive difference in the digital world.

OUR AIM, OBJECTIVE & GOAL

Our primary objective is to empower young leaders by furnishing them with the requisite knowledge and skills essential for navigating the digital realm securely and responsibly. Furthermore, we endeavour to imbue students with leadership attributes aimed at fostering digital citizenship and cultivating a constructive online milieu both for themselves and their respective communities. Our overarching goal is to aid students in maintaining online safety whilst concurrently fostering their capacity to assume leadership roles in advocating exemplary digital conduct within their communities.

TABLE OF CONTENTS

CYBERSECURITY

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at assessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

PURPOSE

Acknowledging the critical role of cyber security in the global economy is essential for safeguarding economic stability, protecting sensitive data, and fostering innovation. The primary goal of cyber security is to protect data. To safeguard data from cyber-attacks, the security sector offers a triangle of three connected principles. The CIA trio is the name for this principle.

OVERVIEW

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks. Cyber security can be described as the collective methods, technologies, and processes to help protect the confidentiality, integrity, and availability of computer systems, networks, and data, against cyber-attacks or unauthorized access.

CYBERSECURITY BASICS

Cybersecurity basics refer to or mean that these are the basics, and everyone SHOULD apply them in their daily life to stay safe from any type of threats, viruses, or cyberbullying! This should be in every person’s daily life.

Firstly, you should use a strong and special password - It should be a combination of uppercase letters, lowercase letters, numbers, and symbols.

Secondly, you should install a firewall because firewalls protect against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet.

Thirdly, you should install an app called **“IDENTIFYING THREATS”** Now what do you mean by this word? This is the process by which a person who might present an insider threat risk due to their observable, concerning behaviours comes to the attention of an organization or insider threat team! Now that we know its meaning we should come to how it helps us consider the threats we identified in light of their likelihood and impact, we can then move towards a deeper analysis of them, the conditions required for them to happen and their potential consequences, which will aid us in planning to react to them.

Fourthly, you should install antivirus apps~ An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop. **(Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them.)**

Fourthly, keep your personal information private avoid sharing your name, address, telephone number, birthday, passwords, and the name of your school when using the Internet Think twice before you post or say anything online; once it is in cyberspace, it's out there forever keep your personal information private avoid sharing your name, address, telephone number, birthday, passwords, and the name of your school when using the Internet Think twice before you post or say anything online; once it is in cyberspace, it's out there forever These are some things to do to avoid cyber bullying

Never post or trade personal pictures. Never reveal personal information, such as address, phone number, or school name or location. Use only a screen name and do not share passwords (other than with parents). Never agree to get together in person with anyone met online without parental approval and/or supervision.

CYBER THREATS

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats also refer to the possibility of a successful Cyber-attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

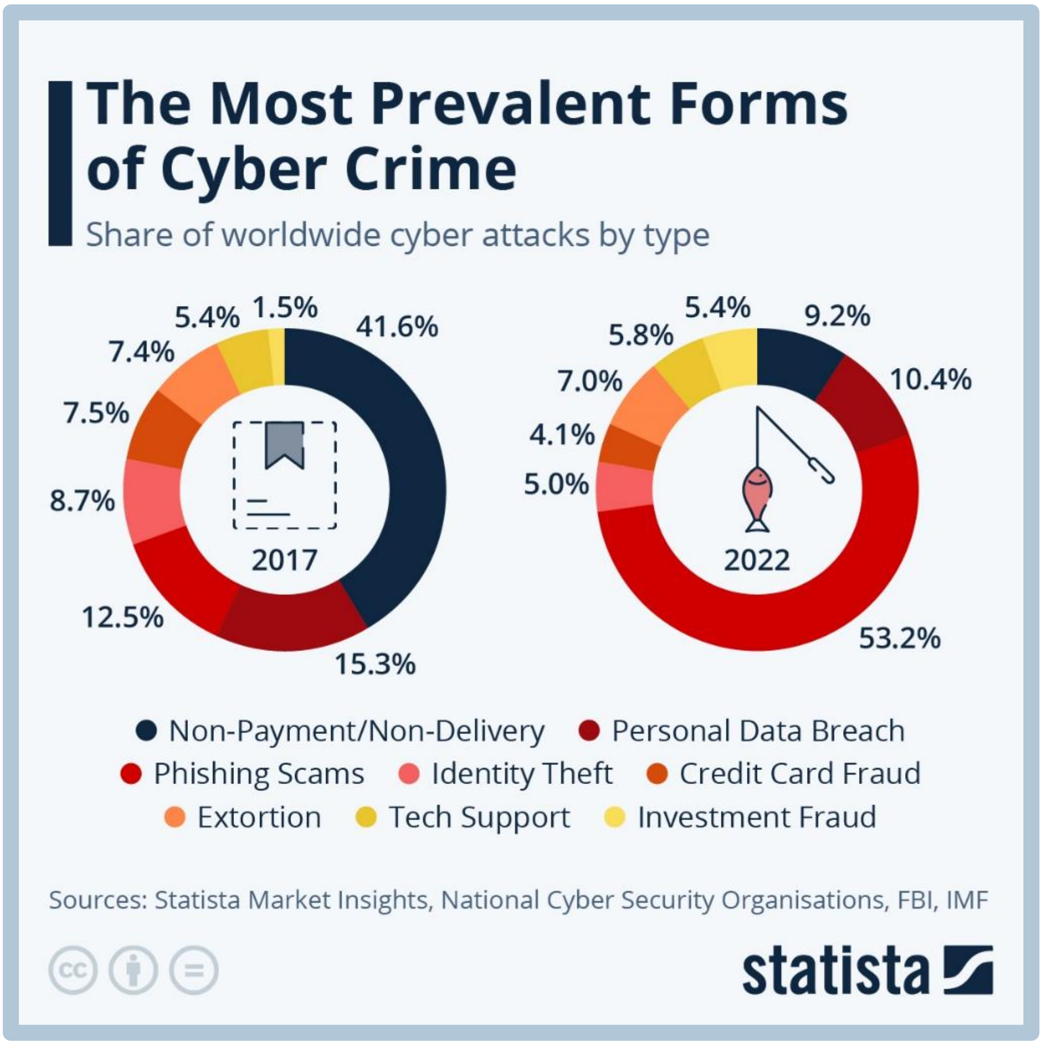
The internet has enabled kids to learn, share and create like never before. But it has also become a space for cybercriminals to cause trouble and steal from others. It is important to instill cyber-secure behaviours from an early age to help children learn how to identify cyber threats and how to mitigate them. -

CYBER ATTACKS YOU SHOULD BE AWARE OF

1. **Phishing:** Scams where attackers send fake emails or messages that look real to trick people into giving away personal information like passwords or credit card numbers.
2. **Ransomware:** Malicious software that locks access to a user's files or system until a ransom is paid, often demanding money for the decryption key.
3. **Malware:** Short for malicious software, it includes viruses, worms, and trojans that can damage systems, steal data, or perform unwanted actions on your computer.
4. **Spyware:** Software that secretly gathers information about a person or organization without their knowledge, often for advertising or malicious purposes.
5. **Adware:** Unwanted software designed to throw advertisements up on your screen, often in a web browser, sometimes hiding spyware.
6. **Trojan Horse:** Malicious software that misleads users of its true intent, often disguised as legitimate software, used by attackers to gain access to systems.
7. **Viruses:** Malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works.
8. **Worms:** Similar to viruses, they can spread across networks without needing to attach themselves to a specific program for distribution.
9. **Man-in-the-Middle (MITM) Attacks:** When attackers secretly relay and possibly alter the communication between two parties who believe they are directly communicating with each other.
10. **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks:** Overwhelm a system’s resources so that it cannot respond to service requests. DDoS is a large-scale attack using multiple computers.
11. **SQL Injection:** A coding vulnerability that allows attackers to interfere with the queries that an application makes to its database, often used to access, and steal data.
12. **Zero-day Exploit:** Attacks that target software vulnerabilities before developers have an opportunity to create a patch to fix them.
13. **Insider Threats:** Threats that come from people within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.
14. **Cryptojacking:** The unauthorized use of someone else’s computer to mine cryptocurrency.

15. **Social Engineering:** The psychological manipulation of people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques.

MOST COMMON FORMS OF CYBERCRIME



The Most Prevalent Forms of Cyber Crime

Share of worldwide cyber attacks by type

Sources: Statista Market Insights, National Cyber Security Organisations, FBI, IMF

IMPACTS OF CYBERATTACKS

CYBERATTACKS ON BUSINESSES AND ORGANIZATIONS

Data Breach: Data loss is a common impact of a cyberattack. Cybercriminals commonly target customer data, intellectual property (IP), financial data, and other sensitive information in their attacks.

Denial of Service (DoS): Some cyberattacks are designed to disrupt an organization's operations. For example, a distributed denial-of-service (DDoS) attack might overwhelm a web server with spam traffic, or ransomware might encrypt vital data, rendering it unavailable to an organization.

Financial Losses: Most cyberattacks cause a variety of financial losses. Even if the cybercriminals do not steal money directly, an organization may face remediation costs, legal fees, and lost revenue because of a cyberattack.

Reputational Damage: A successful cyber-attack can also cause considerable damage to an organization's brand image. The company's reputation may be harmed by customers' perception that the organization cannot protect their data or the inability to provide core services during a DoS attack.

Customer Losses: Cyberattacks can also cause an organization to lose customers. This customer churn could be caused by customers' inability to reach an organization's website during a DDoS attack or a company's perceived failure to properly protect customer data.

CYBERATTACKS ON INDIVIDUALS

Financial Loss: Cyberattacks can lead to direct financial loss through fraudulent transactions, theft of banking details, or extortion via ransomware. Victims may find unauthorized charges on their accounts or lose access to their digital wallets.

Identity Theft: Personal information obtained through cyberattacks can be used to impersonate victims, leading to identity theft. This can result in unauthorized activities under the victim's name, such as applying for loans, making purchases, or committing crimes.

Emotional and Psychological Stress: Falling victim to a cyberattack can induce significant emotional distress, including feelings of violation, embarrassment, anxiety, and depression. The invasion of personal privacy and the potential public exposure of private information can have long-lasting psychological effects.

Damage to Reputation: Cyberattacks that result in the release of personal or sensitive information can harm an individual's reputation. This could impact personal relationships, professional standing, and future opportunities.

Loss of Data: Attacks such as ransomware or data breaches can lead to the loss of valuable personal data, including photos, documents, and other irreplaceable files. This loss can have sentimental as well as practical implications.

Recovering from a cyberattack often requires significant time and effort, disrupting daily activities. Victims may need to spend time restoring accounts, changing passwords, and repairing damaged files, which can be both time-consuming and frustrating.

Legal and Regulatory Consequences: Victims of cyberattacks may find themselves entangled in legal and regulatory issues, especially if their stolen information is used for illegal activities. Navigating these challenges can be complex and require legal assistance.

Decreased Trust in Digital Systems: Experiencing a cyber-attack can lead individuals to lose trust in digital platforms and services. This skepticism may hinder their engagement with online services, impacting their personal and professional efficiency.

Long-Term Security Concerns: Once personal information is compromised, individuals may face ongoing security risks. Cybercriminals can continue to use or sell the information, leading to a prolonged period of vulnerability.

ONLINE SCAMS

Reporting fraud promptly is crucial to prevent further harm and to help authorities take action against scammers.

Phishing Scams:

- Description: Phishing scams involve sending fraudulent emails or messages to trick recipients into revealing sensitive information such as passwords, credit card numbers, or personal details.
- Identification: Look for suspicious email addresses, grammatical errors, urgent requests for personal information, and unfamiliar links.
- Reporting: Report phishing emails to the Anti-Phishing Working Group (APWG) or the company being impersonated.

Tech Support Scams:

- Description: Tech support scams involve imposters posing as technical support representatives who claim that your device has issues and offer fake solutions or services for a fee.
- Identification: Be wary of unsolicited calls or pop-up messages claiming technical problems, especially if they ask for remote access or payment details.
- Reporting: Report tech support scams to the Federal Trade Commission (FTC) or your country's consumer protection agency.

Online Shopping Scams:

- Description: Online shopping scams occur when fake websites or sellers deceive consumers by selling counterfeit or nonexistent products, or by not delivering purchased items.
- Identification: Check for secure website connections (https://), read customer reviews, verify seller information, and be cautious of deals that seem too good to be true.
- Reporting: Report online shopping scams to your country's consumer protection agency or to platforms like the Better Business Bureau (BBB).

Investment Scams:

- Description: Investment scams lure victims into fake investment opportunities promising high returns, but they often result in financial losses as the investments are non-existent or fraudulent.
- Identification: Research investment opportunities thoroughly, be skeptical of guaranteed high returns, and verify the legitimacy of investment firms or platforms.
- Reporting: Report investment scams to the Securities and Exchange Commission (SEC) or your country's financial regulatory authority.

Social Media Scams:

- Description: Social media scams involve fraudulent activities such as fake giveaways, phishing links, or impersonation profiles that aim to trick users into sharing personal information or clicking on malicious links.

- Identification: Be cautious of unusual messages or friend requests from unknown users, verify official accounts before engaging, and avoid clicking on suspicious links or providing personal information online.
- Reporting: Report social media scams to the platform's support or reporting tools, such as Facebook's "Report" feature or Twitter's "Report Tweet" option. You can also notify your parents or guardians and seek help from them.

TYPES OF CYBER-SECURITY

Cyber security is a wide field covering several disciplines. It can be divided into seven main pillars:

1. **Network Security**

   Most attacks occur over the network, and network security solutions are designed to identify and block these attacks. These solutions include data and access controls such as Data Loss Prevention (DLP), IAM (Identity Access Management), NAC (Network Access Control), and NGFW (Next-Generation Firewall) application controls to enforce safe web use policies.

   Advanced and multi-layered network threat prevention technologies include IPS (Intrusion Prevention System), NGAV (Next-Gen Antivirus), Sandboxing, and CDR (Content Disarm and Reconstruction). Also important are network analytics, threat hunting, and automated SOAR (Security Orchestration and Response) technologies.

2. **Cloud Security**

   As organizations increasingly adopt cloud computing, securing the cloud becomes a major priority. A cloud security strategy includes cyber security solutions, controls, policies, and services that help to protect an organization's entire cloud deployment (applications, data, infrastructure, etc.) against attack. Many cloud providers offer security solutions; these are often inadequate for the task of achieving enterprise-grade security in the cloud. Supplementary third-party solutions are necessary to protect against data breaches and targeted attacks in cloud environments.

3. **Endpoint Security**

   The zero-trust security model prescribes creating micro-segments around data wherever it may be. One way to do that with a mobile workforce is using endpoint security. With endpoint security, companies can secure end-user devices such as desktops and laptops with data and network security controls, advanced threat prevention such as anti-phishing and anti-ransomware, and technologies that provide forensics such as endpoint detection and response (EDR) solutions.

4. **Mobile Security**

   Often overlooked, mobile devices such as tablets and smartphones have access to corporate data, exposing businesses to threats from malicious apps, zero-day, phishing, and IM (Instant Messaging) attacks. Mobile security prevents these attacks and secures the operating systems and devices from rooting and jailbreaking. When included with an MDM (Mobile Device Management) solution, this enables enterprises to ensure only compliant mobile devices have access to corporate assets.

5. **IoT Security**

   While using Internet of Things (IoT) devices certainly delivers productivity benefits, it also exposes organizations to new cyber threats. Threat actors seek out vulnerable devices inadvertently connected to the Internet for nefarious uses such as a pathway into a corporate network or for another bot in a global bot network.

   IoT security protects these devices with the discovery and classification of the connected devices, auto-segmentation to control network activities, and using IPS as a virtual patch to prevent exploits against vulnerable IoT devices. In some cases, the firmware of the device can also be augmented with small agents to prevent exploits and runtime attacks.

6. **Application Security**

   Web applications, like anything else directly connected to the Internet, are targets for threat actors. Since 2007, OWASP has tracked the top ten threats to critical web application security flaws such as injection, broken authentication, misconfiguration, and cross-site scripting to name a few.

   application security, the OWASP Top 10 attacks can be stopped. Application security also prevents bot attacks and stops any malicious interaction with applications and APIs. With continuous learning, apps will remain protected even as DevOps releases updated content.

7. **Zero Trust**

   The traditional security model is perimeter-focused, building walls around an organization’s valuable assets like a castle. However, this approach has several issues, such as the potential for insider threats and the rapid dissolution of the network perimeter.

CYBERSECURITY ETHICS

Cybersecurity ethics refers to the moral principles and guidelines that govern the behaviour of individuals and organizations in the context of cyber environments and information technology. Given the increasing reliance on digital technologies in almost all aspects of life, ethical considerations in cybersecurity have become critically important. These ethical guidelines help in making decisions about what is right or wrong in the creation, sharing, and protection of information on the Internet and other digital platforms.

Key areas of concern in cybersecurity ethics include:

Privacy: Balancing the need for security with respecting individuals' right to privacy is a central ethical challenge. This includes questions about data collection, surveillance, and the extent to which personal information should be protected or can be shared.

Data Protection and Integrity: Ensuring the accuracy, reliability, and safety of data. This involves protecting data from unauthorized access, destruction, or alteration. Ethical practices include implementing strong security measures and respecting the confidentiality of information.

Access: Ethical considerations about who has the right to access information and technology. This includes bridging the digital divide and ensuring equitable access to technology, as well as making decisions about the distribution of resources and capabilities.

Transparency and Accountability: Maintaining openness about cybersecurity policies, practices, and breaches, and being accountable for security failures. Organizations should be transparent about their data handling and protection practices, and individuals should be held accountable for their actions in cyberspace.

Consent: Ensuring that individuals have control over their personal information and are informed about how their data is being used. This includes obtaining explicit consent before collecting, using, or sharing someone's data.

Ethical Hacking: The practice of breaking into systems to find and fix security vulnerabilities. Ethical hackers, or white-hat hackers, operate under a code of ethics that includes permission from the rightful owners before attempting to breach systems.

International Cooperation: Cybersecurity is a global issue that requires cooperation across borders. Ethical considerations include respecting international norms and working together to combat cyber threats without infringing on national sovereignties.

Ethical decision-making in cybersecurity is complex and often involves navigating difficult trade-offs. Ethical guidelines and frameworks help individuals and organizations to make informed decisions that not only comply with legal standards but also respect the broader social and moral obligations of operating in a digitally interconnected world.

DIGITAL CITIZENSHIP

What is digital citizenship?

Digital citizenship refers to the responsible use of technology by anyone who uses computers, the internet, and digital devices to engage with society on any level. It is about understanding and upholding ethical, respectful, and safe behaviours in the digital environment. Digital citizenship encompasses several key aspects, including:

1. **Digital Literacy:** Understanding how to use technology and the internet effectively, including the ability to evaluate and integrate digital resources into daily tasks.
2. **Digital Etiquette:** Practicing respect and courtesy in online interactions. This includes understanding the implications of online behaviour and recognizing the impact it can have on others.
3. **Digital Law:** Abiding by laws and policies that govern digital spaces, including respecting copyright and intellectual property rights, and understanding the legal implications of digital actions.
4. **Digital Rights and Responsibilities:** Recognizing and respecting the rights of all digital users, including privacy and freedom of expression, while also acknowledging the responsibilities that come with those rights, such as respecting the privacy of others.
5. **Digital Health and Wellness:** Understanding the physical and psychological impacts of digital technology usage, such as practicing ergonomic principles while using devices, and being aware of the potential for digital addiction.
6. **Digital Security (Self-Protection):** Taking initiative-taking steps to protect personal information and data from cyber threats, such as using strong passwords, being wary of suspicious links or emails, and regularly updating software.
7. **Digital Communication:** Effectively communicating and collaborating with others using digital technologies, understanding the power of digital platforms, and using them to create positive and constructive dialogues.
8. **Digital Footprint and Reputation:** Being aware that digital activities are often recorded and can form a lasting digital footprint, impacting one's reputation now and in the future.
9. **Digital Commerce:** Understanding the economic implications of digital transactions and the potential risks and benefits of online shopping, banking, and investments.

Embracing good digital citizenship helps create a safer, more respectful, and more collaborative online community. It empowers users to navigate digital spaces wisely, make informed decisions and engage positively in the digital world.

Rules of digital citizenship:

1. Use appropriate language and behaviour when interacting with others (i.e., cyberbullying).
2. Respect the opinions and ideas of others.
3. Obey all intellectual property laws.
4. Do not use or share others' work without permission.
5. Follow rules and/or codes of conduct for every Internet site.

RESPECTING OTHERS ONLINE

Why is it important to be respectful online?

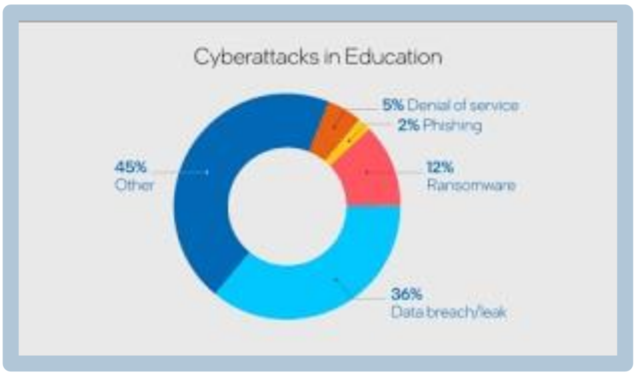
Being respectful online is important because it helps create a positive environment where everyone can communicate safely. Without seeing each other face-to-face, it is easier to misunderstand or hurt others with our words. By being kind and considerate, we can avoid spreading negativity and make the internet a better place for everyone. This also prevents cyberbullying and supports good mental health. Simply put, being respectful online sets a good example and encourages others to act the same way, making our online communities friendlier for everyone.

Ways to be respectful online:

1. Respect the fact that everyone can have a different opinion of you.
2. If you cannot be positive and helpful, then do not comment just to pull someone else down.
3. Never think you are better than anyone.
4. Do not argue on social media.
5. Do not post anything that will upset anyone else.

CYBERSECURITY IN EDUCATION

WHY IS CYBERSECURITY IMPORTANT IN EDUCATION?



Cybersecurity is crucial in any business setting, but especially in education. Cyberattacks not only compromise the safety and security of teachers and school administrations but also the privacy of students—particularly minors in K–12 institutions. Today millions of students are learning through technology in hybrid, remote, or in-class environments, which is why keeping their devices secure is paramount for students' learning experiences and teachers' work.

COMMON CYBER INCIDENTS

The educational sector saw an incredible rise in cyberattacks during the COVID-19 pandemic as more people started using connected devices for school. K12 schools endured a variety of incidents, from ransomware to data breaches to phishing.1

A graph showing the types of cyberattacks that impact education environments.

Note: "Other" includes malware, meeting invasions, and website and social media defacement.

These additional statistics only brush the surface on why cybersecurity is so important in education.

One in three education devices contains sensitive data.2

In a study of 5,400 IT decision-makers across thirty countries, education sectors are the most likely to admit security weaknesses.3

Forty-four percent of IT managers in the education sector experienced a ransomware attack. This is the highest level of attack compared to a variety of other industries such as healthcare, IT, and local government.4

Eighty-seven percent of educational establishments have experienced at least one attack.5

Among all industries, the education sector is one of the least secure, and schools are the second most lucrative target for ransomware.6

Cybersecurity in K–12 and Higher Education

Cybersecurity varies slightly between K–12 and higher education but is equally important. Keeping student information secure is especially vital for those under the age of eighteen in K–-12 institutions. While the Family Educational Rights and Privacy Act (FERPA) of 1974 protects student records, it does not require K–12 schools to adopt specific security protocols. Some states have individual laws that protect students online, like the Student Online Personal Information Protection Act (SOPIPA) in the United States, seven but these laws are not enforced at a federal level, often leaving an individual school district's IT staff to protect student and teacher data and privacy.

In higher education, students and faculty usually bring their own devices, which require additional security and individual due diligence. Students and faculty have to not only think about keeping their data safe but feel confident in their institution, keeping their privacy secure as well. This is also especially important for students and teachers who travel around campus and get their work done on and off campus, like in off-site research labs.

HOW TO INCREASE SAFETY

There are a few ways IT professionals in education can protect students from cyber criminals. For younger students, having good security hygiene can help keep them safe from a cyberattack. However, being able to spot scams can only help protect students so much, which is why IT staff should look into using devices with hardware-based security features or even adopting a Device as a Service (DaaS) management system.

PROPER SECURITY HYGIENE

Most adult users know not to click a suspicious link or put an unfamiliar USB flash drive into their devices, but younger students do not always know better. Teaching younger students about cyber risks at an early age can lower their chances of getting attacked or hacked by a cybercriminal. Intel IT Information Security created the Online Safety for Kids program with this in mind. The program aims to encourage kids to learn about cyber risks with presentations, parent information, and quizzes that are appropriate for any students from age five and up.

HARDWARE-BASED SECURITY

Most industries—education included—rely on security software to protect themselves and their assets, but a hacker can also exploit vulnerabilities below the operating system (OS). Hardware-based security not only protects devices at the software level but also helps prevent malware injections below the OS. Hardware-based security shrinks the attack surface, which is any vector that an attacker can use to gain access to or compromise data. With hardware-based security severely limiting or eliminating the options for a potential attack, if a student accidentally clicks a bad link, their chance

s of staying protected increase.
The Intel vPro® platform offers several exclusive hardware-based security features like Intel® Active Management Technology (Intel® AMT) with Intel® Endpoint Management Assistant and Intel® Threat Detection Technology. These advanced, full-stack security features can help protect end-user devices, data, and productivity, giving students, teachers, and IT staff peace of mind.

DEVICE AS A SERVICE (DaaS)

IT staff know that technology is meant to function as an enabler of learning rather than a barrier, and DaaS solutions enabled by Intel vPro® can do exactly that. With DaaS, a third-party solution provider equips schools with all the end-user devices they need, packaged with full remote device management and technical support. And with the Intel vPro® platform, DaaS customers get advanced hardware-based security with Intel® Hardware Shield. This frees up resources for the school’s IT staff, so they can focus on digital transformation projects that enable rich learning environments.

COPYRIGHT LAWS

Understanding copyright laws:

Copyright laws grant creators exclusive rights over their original works, such as literary, artistic, musical, or dramatic creations. These rights include the right to reproduce the work, distribute copies, perform, or display the work publicly, and create derivative works. Copyright protection automatically applies to qualifying works upon their creation, without the need for registration or any other formalities. However, registration may be necessary to enforce copyright in some authorities.

Respecting intellectual property rights:

Respecting intellectual property rights entails acknowledging and honouring the legal rights of creators and owners of intellectual property. This involves obtaining permission or licensing when using copyrighted materials, giving proper attribution to the creators, and refraining from unauthorized use, reproduction, or distribution of protected works. Respecting intellectual property rights fosters a culture of creativity, innovation, and fair compensation for creators and contributes to the overall advancement of society.

Fair use guidelines for using and sharing content:

Fair use is a legal doctrine that allows for the limited use of copyrighted material without permission from the copyright owner under certain circumstances, such as for purposes of criticism, commentary, news reporting, teaching, scholarship, or research. Fair use considers factors such as the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used, and the effect of the use on the potential market for or value of the copyrighted work. However, determining whether a particular use qualifies as fair use can be complex and may require legal analysis on a case-by-case basis.

Creating original work and giving credit to others:

Creating original work involves generating new and innovative content that is not substantially similar to existing works. Originality is a key criterion for copyright protection, and creators are encouraged to develop unique expressions of ideas. Additionally, giving credit to others involves acknowledging the contributions of individuals or sources that have influenced or contributed to one's work. Proper attribution not only respects the intellectual property rights of others but also promotes transparency, integrity, and collaboration within creative communities.

FIREWALLS

Firewalls are a fundamental component of network security. They function as a barrier between a trusted internal network and untrusted external networks, such as the Internet. A firewall can be either software or hardware, and its primary purpose is to regulate the traffic between these networks based on an organization's or individual's security policies. Here is a more detailed look at key aspects of firewalls:

TYPES OF FIREWALLS

Packet-Filtering Firewalls: The most basic type, which inspects packets (small chunks of data) travelling across the network. It makes decisions to allow or block these packets based on predefined rules, like IP addresses, protocol, and ports.

Stateful Inspection Firewalls: Also known as dynamic packet filtering, this type monitors the state of active connections and makes decisions based on the context of the traffic and the state of the connection, in addition to the static rules.

Proxy Firewalls (Application-Level Gateways): These function as an intermediary between users and the internet. They filter incoming and outgoing data at the application layer, providing detailed, protocol-aware filtering.

Next-Generation Firewalls (NGFW): These combine the capabilities of the traditional firewall with additional functionalities, such as encrypted traffic inspection, intrusion prevention systems (IPS), and identity-based access control. They are designed to address the more sophisticated threats in today's cybersecurity landscape.

Network Address Translation (NAT) Firewalls: These hide the true IP addresses of computers on a network by assigning a public IP address to all outgoing traffic. This not only conserves the number of IP addresses used but also adds a layer of anonymity to the network's devices.

KEY FUNCTIONS

Traffic Control: Regulate incoming and outgoing network traffic based on an organization's security policy.

Protection from Threats: Help protect networks from threats like worms, malware, and other unwanted traffic that could compromise security.

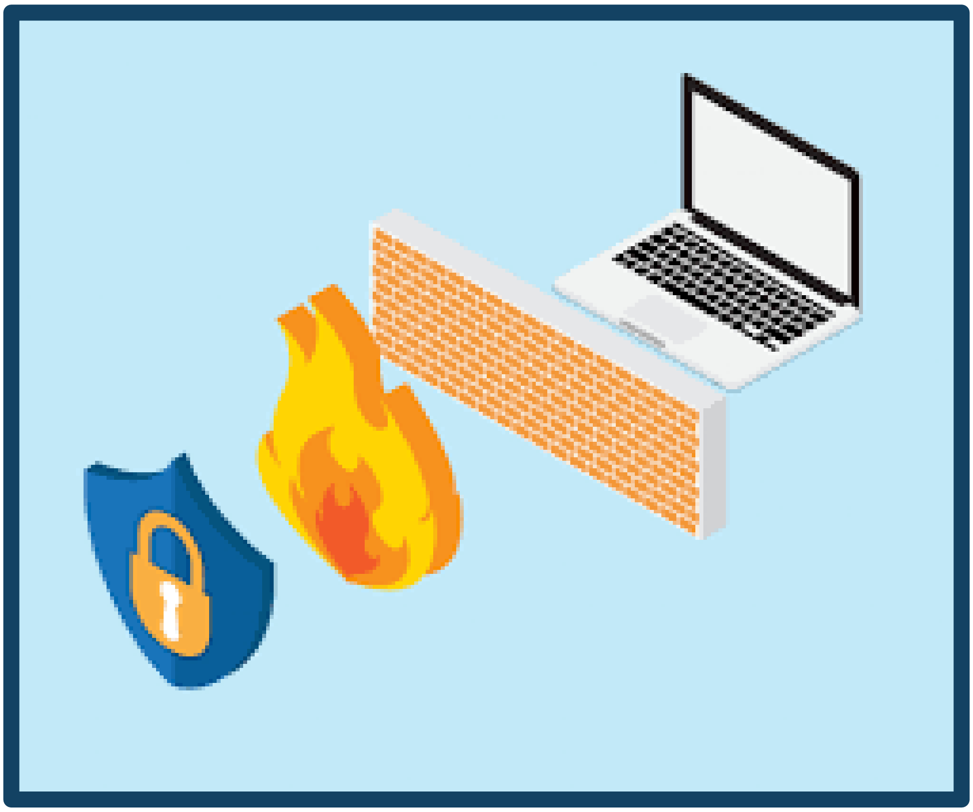
Logging and Reporting: Keep detailed logs of network activity and generate reports on traffic patterns, attempted breaches, or other security events.

DISADVANTAGES OF FIREWALLS

Complexity: As network environments become more complex, managing firewall rules and configurations can become challenging.

Performance: High levels of security may impact network performance, so balance is crucial.

Evolving Threats: Firewalls need to be updated and configured properly to protect against evolving cybersecurity threats. configurations can become challenging.
defence against potential external threats. However, they should be complemented with other security measures to ensure a robust security posture.



TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) is a security process that requires users to provide two different types of information before gaining access to an online account or system. This method adds an extra layer of security beyond just a password, making it significantly harder for unauthorized individuals to breach accounts. The rationale behind 2FA is that even if a hacker manages to obtain your password, they will still need the second factor to access your account, which they typically will not have.

HOW IT WORKS

When you enable 2FA on an account, you are required to go through two verification steps to prove your identity:

Something You Know: This is usually your password. It is the first factor and something only you should know.
Something You Have: This is the second factor, and it can be a variety of things:

- A text message (SMS) code sent to your phone.
- A code generated by an authentication app (like Google Authenticator, Authy, or Microsoft Authenticator).
- A hardware token that generates a code at the push of a button.
- A biometric factor like your fingerprint, voice, or facial recognition.

TYPES OF TWO-FACTOR AUTHENTICATION

SMS and Email Codes: A code sent to your phone or email. While convenient, it is considered less secure than other methods because of the potential for SIM swapping or email account breaches.
Authentication Apps: Generate time-sensitive codes. Since they are tied to your physical device (like a smartphone), they are more secure than SMS codes.
Hardware Tokens: Small physical devices that generate a new code at the push of a button. They are considered very secure but can be less convenient since you must carry the token with you.
Biometric Methods: Use unique biological characteristics such as fingerprints or facial recognition. They offer a high level of security and convenience, assuming the system accurately detects the user.

BENEFITS

Enhanced Security: Significantly reduces the risk of unauthorized access, even if a password is compromised.
User Confidence: Increases user confidence in the security of their accounts and sensitive information.
Compliance: Helps organizations comply with security regulations and standards that require 2FA.

DISADVANTAGES

While 2FA enhances account security, it is fallible. Users should remain vigilant about phishing attempts designed to steal 2FA codes and should use the most secure 2FA method available to them. Despite its minor inconveniences, such as needing access to a phone or another device, the benefits of added security make 2FA a crucial tool in protecting online accounts.

PASSWORD MANAGEMENT

Password management is a critical aspect of digital security, involving the creation, storage, and organization of passwords. Here is a comprehensive overview covering various facets of password management:

IMPORTANCE OF PASSWORD MANAGEMENT

Security: Proper password management helps protect accounts from unauthorized access, data breaches, and cyberattacks.
Privacy: Ensures personal and sensitive information remains confidential.
Convenience: Simplifies the process of handling multiple passwords, reducing the burden of remembering complex combinations.

BEST PRACTICES

Use Strong Passwords: Create long passwords (12 characters minimum), and include a mix of letters, numbers, and special characters.
Unique Passwords: Use a different password for every account to prevent a single breach from compromising multiple accounts.
Password Updates: Regularly update passwords, especially for sensitive accounts like email and banking.
Two-Factor Authentication (2FA): Whenever possible, enable 2FA to add an extra layer of security.
Avoid Common Pitfalls: Do not use easily guessable information like birthdays, names, or common words.

PASSWORD MANAGEMENT TOOLS

Password managers are software tools that help in creating, storing, and managing passwords securely. Key features and benefits include:
Secure Storage: Encrypt and store passwords in a secure vault, accessible with an expert password.
Password Generation: Automatically generate strong, random passwords.
Autofill: Automatically fill in usernames and passwords, reducing the risk of phishing.
Cross-Platform: Most managers are available across different devices and platforms, ensuring access to your passwords anywhere.
Secure Sharing: Some password managers allow the secure sharing of passwords with trusted individuals.

POPULAR PASSWORD MANAGERS

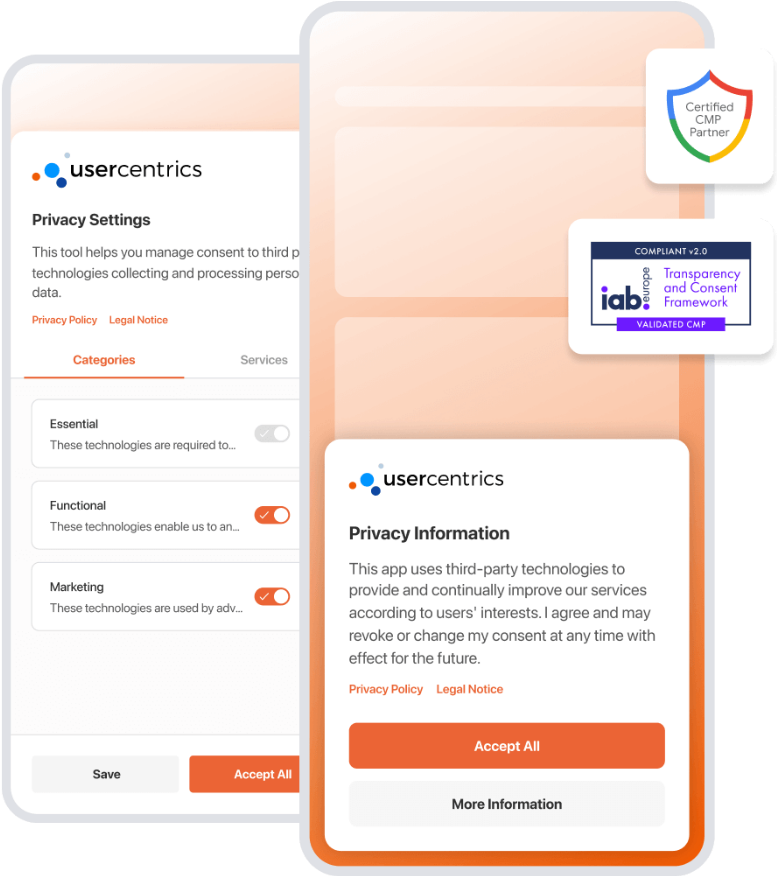
Several reputable password managers are available, each with its own set of features. Popular options include:
LastPass, 1Password, Dashlane, & Bitwarden

PRIVACY SETTINGS AND MANAGEMENT

Understanding and managing privacy settings on social media and other online platforms is crucial for protecting personal information from unauthorized access. This section explores the importance of privacy settings and offers practical advice on how to manage them effectively.

Key Points:

1. **The Importance of Privacy Settings:** Explains why privacy settings are essential for safeguarding personal information and outlines the potential risks of leaving personal data exposed.
2. **Navigating Privacy Settings:** Offers step-by-step guidance on accessing and adjusting privacy settings on popular social media platforms and online services to control who sees your information.
3. **Best Practices for Online Privacy:** Provides tips for maintaining privacy online, including being cautious about the information shared on social media, understanding default privacy settings, and regularly reviewing privacy preferences.
4. **Tools and Resources:** Introduces tools and resources that can help users manage their online privacy more efficiently, such as privacy check-up features provided by social media platforms.



Privacy Settings

This tool helps you manage consent to third p technologies collecting and processing perso data.

Essential — These technologies are required to...

Functional ✓ — These technologies enable us to an...

Marketing ✓ — These technologies are used by adv...

Privacy Information

This app uses third-party technologies to provide and continually improve our services according to users' interests. I agree and may revoke or change my consent at any time with effect for the future.

SECURE WI-FI NETWORKS

Wi-Fi networks are gateways to the internet but can also be vulnerable if not properly secured. This section discusses the importance of securing Wi-Fi networks at home and in public spaces and offers guidelines for using VPNs to enhance security.

Key Points:

1. **Securing Home Wi-Fi Networks:** Details steps to secure home Wi-Fi networks, including changing the default router password, enabling WPA2 or WPA3 encryption, and hiding the network from public view.
2. **Risks of Public Wi-Fi:** Outlines the security risks associated with using public Wi-Fi networks, such as the potential for eavesdropping and data interception by cybercriminals.
3. **Using VPNs on Public Wi-Fi:** Explains what a VPN (Virtual Private Network) is and how it can protect your data by encrypting internet traffic, making it much harder for hackers to access your information on public Wi-Fi.
4. **Best Practices for Wi-Fi Security:** Offers a list of best practices for Wi-Fi security, including regularly updating router firmware, disabling WPS (Wi-Fi Protected Setup), and using a guest network for visitors.
5. **By addressing these two critical aspects of cybersecurity, users can significantly enhance their online privacy and security, reducing the risk of unauthorized access and cyber threats.**

HOW TO STAY SAFE ONLINE

Staying safe online is crucial in today's digital age, where cybersecurity threats are constantly evolving. Here are some key strategies to help you protect yourself and your information:

Use Strong Passwords: Create complex passwords that are hard to guess. Use a combination of letters, numbers, and symbols, and avoid using the same password for multiple accounts. Consider using a password manager to keep track of your passwords.
Enable Two-Factor Authentication (2FA): Whenever possible, enable 2FA on your accounts. This adds an extra layer of security by requiring not only your password but also a code sent to your phone or email.
Keep Your Software Updated: Regularly update your operating system, browsers, and any installed software to patch security vulnerabilities. Enable automatic updates if available.
Be Wary of Phishing Attempts: Phishing emails or messages try to trick you into giving away personal information. Always verify the source before clicking on links or downloading attachments. Be skeptical of emails requesting urgent action or personal information.
Use Secure Connections: When browsing online, look for the "HTTPS" in the URL, indicating a secure connection. Avoid using public Wi-Fi for sensitive transactions or use a Virtual Private Network (VPN) to encrypt your internet connection.
Backup Your Data: Regularly backup important data to an external hard drive or cloud storage. This ensures you have a copy of your information in case of cyber-attacks like ransomware.
Use Privacy Settings: Review and adjust the privacy settings on your social media and other online accounts. Limit the amount of personal information you share publicly.
Install Antivirus Software: Use reputable antivirus software to protect your devices from malware and other threats. Keep the software up to date.
Be Mindful of What You Share Online: Think twice before posting personal information online. Information shared on the internet can often be seen by unintended audiences and could be used against you.
Educate Yourself: Stay informed about the latest cybersecurity threats and best practices for online safety. Knowledge is a powerful tool for protecting yourself online.

By following these tips, you can significantly reduce your risk of falling victim to online threats and ensure a safer browsing experience.

WHAT TO DO IF YOU ARE CYBERBULLIED

If you find yourself a victim of cyberbullying, it is crucial to know that help is available and that you are not alone. Here is a step-by-step guide on how to handle the situation:

1. **Do not Retaliate:** Responding to bullies can often make the situation worse. Try to stay calm and avoid engaging with the bully.
2. **Keep the Evidence:** Save messages, pictures, or any other evidence of cyberbullying. This can be important if the situation escalates, and you need to show what has been happening.

3. **Tell Someone You Trust**: Whether it is a parent, friend, teacher, or counsellor, it is important to talk to someone about what you are experiencing. They can offer support and advice on the next steps.
4. **Block the Bully**: Most social media platforms and messaging apps allow you to block users who are harassing you. This can prevent them from contacting you further.
5. **Report the Bullying**: Report the cyberbullying to the platform where it occurred. Most websites and apps have policies against bullying and can take action against the users involved. If bullying involves threats of violence, extortion, or sexual images, consider reporting it to law enforcement.
6. **Adjust Privacy Settings**: Review your privacy settings on social media and other online platforms. Limiting who can see your posts and contact you can help prevent future incidents.
7. **Seek Professional Help**: Cyberbullying can have a significant emotional impact. If you are feeling overwhelmed, anxious, or depressed, talking to a counsellor or therapist can help you cope with your feelings.
8. **Educate Yourself and Others**: Understanding more about cyberbullying and sharing this knowledge can help you and others feel more empowered to deal with it. Schools and communities often have resources and programs aimed at preventing bullying.
9. **Take Care of Yourself**: Make sure to engage in activities that you enjoy and that help you relax. Spending time with friends, practicing hobbies, or exercising can improve your mood and help you cope with stress.
10. **Know Your Rights**: In some cases, cyberbullying can cross the line into criminal behaviour. It is important to know that there are laws in many regions designed to protect victims of cyberbullying. Consulting with a legal professional can guide your options.

WHAT TO DO IF YOU ARE HACKED OR SCAMMED

If you have been hacked or scammed, acting quickly can help mitigate the damage and secure your information. Here are essential steps to take immediately after you realize you have been compromised:

1. **Change Your Passwords:** Start by changing the passwords for any accounts that may have been compromised, as well as any accounts that use a similar password. Use strong, unique passwords for each account, and consider using a password manager to keep track of them.
2. **Enable Two-Factor Authentication:** For added security, enable two-factor authentication (2FA) on your accounts, especially for your email, banking, and social media accounts. This adds an extra layer of protection by requiring a second form of verification.
3. **Alert Your Bank and Credit Card Companies:** If your financial accounts have been hacked or you have been scammed out of money, contact your bank and credit card companies immediately to report the fraud. They can monitor your accounts for suspicious activity and help protect your money.
4. **Check Your Computer for Malware:** Run a full scan of your computer with updated antivirus software to check for any malware or viruses that may have been installed. Ensure your antivirus software and operating system are up to date to prevent future attacks.

5. **Report the Incident:** Report the hacking or scam to the appropriate authorities. This could include your local police department, the Federal Trade Commission (FTC) in the U.S., or the relevant consumer protection agency in your country. If the scam involves your online accounts, report the incident to the service provider.
6. **Monitor Your Accounts and Credit Reports:** Keep an eye on your financial statements and online accounts for any unauthorized transactions or changes. Additionally, monitor your credit report for unexpected changes that could indicate identity theft. In some countries, you can set up fraud alerts or credit freezers.
7. **Secure Your Email:** If your email account has been compromised, secure it by changing the password and security questions. Email accounts are often targeted because they can be used to reset passwords for other accounts.
8. **Educate Yourself About Scams**: Familiarize yourself with common types of scams to better protect yourself in the future. Understanding how scammers operate can help you spot and avoid scams.
9. **Warn Your Contacts:** If your email or social media accounts have been hacked, notify your contacts that they may receive phishing messages from your account. Advise them not to click on any suspicious links.
10. **Document Everything:** Keep records of all communications related to hacks or scams, including any reports you file. This documentation can be important if you need to prove the incident occurred or seek restitution.

STATISTICAL DATA

The cybersecurity landscape is continuously evolving. And now with COVID-19, remote work, and increasing cybercrimes in the picture, maintaining fool-proof security is becoming harder and harder.

To give you a better view of what is happening with cybersecurity, we curated a list of 160 cybersecurity stats for 2024.

FORECASTS FOR CYBERSECURITY IN 2024

Did you know a cyberattack happens every 39 seconds? That is less time than it takes to order takeout. To put this in perspective, cybercrime is predicted to cost the world USD 9.5 trillion in 2024.

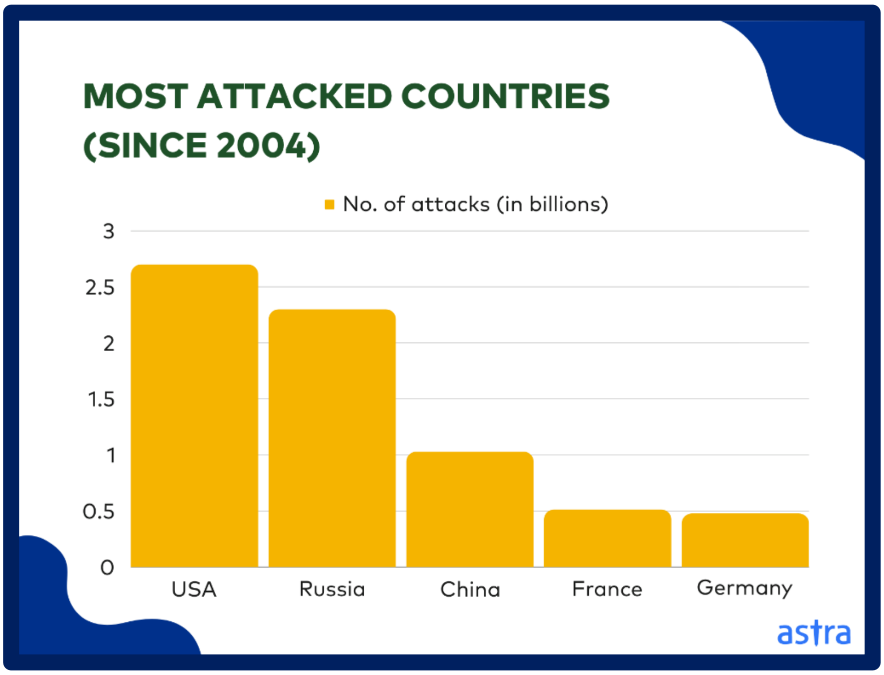
This staggering amount underscores the imminent need for cyber security to be treated as a global priority. Moreover, with the explosion of generative AI (besides chatGPT as well!), the current 2200 daily attacks, are expected to not only multiply manifold but become far more individualized.

Despite modern technology, ransomware will possibly continue to dominate cybercrime in 2024. In fact, according to Statista, it was the leading motive for more than 72% of cybersecurity in 2023.

Moreover, even with the widespread impact, small and medium-sized businesses (SMBs) seem to be the new bullseye, as documented by 61% of SMBs that were hit in 2023. As such, the expected growth of the global cybersecurity market to $266.2 Billion by 2027, hardly comes as a surprise.

As such, with the alarming 8.9% CAGR of the cybersecurity industry, Gartner predicts, that 50% of C-suite leaders will have cybersecurity risk-related performance requirements embedded in their contracts by 2026.

TOP 5 COUNTRIES BY CYBERCRIME DENSITY



HEADLINES FOR CYBERSECURITY 2023

At the time of writing, 28778 new vulnerabilities have been discovered in 2023 alone, dwarfing 2022's total vulnerabilities by nearly 3700+. In fact, at the current rate of 14.8%, 2024 will have 33K+ CVEs.

Conversely, recent research by the World Economic Forum reveals a striking lack of confidence among organizations. Only 4% of organizations are confident in their assurance of security to "users of connected devices and related technologies are protected against cyberattacks."

This unfortunately indicates that most organizations (federal and private) have adopted a reactive rather than initiative-taking approach to cybersecurity i.e., they place damage control campaigns on a higher priority than preventative vigilance.

Simply put, Fortra's reactive stance allowed hackers to exploit a zero-day vulnerability and trigger a domino effect for 130+ companies. In contrast, Google's initiative-taking measures successfully defended against a massive DDoS attack, handling over 398 million requests per second.

Adding to the shocking news, IBM's 2023 report indicates the average cost of a corporate data breach in 2023 stood at $4.45 million. However, supply chain attacks can far exceed such a cost, especially in the case of key APIs.

The infamous MOVEit Supply Chain Attack in June was plenty of proof, as it managed to compromise more than 620 organizations including bigwigs such as BBC and British Airways.

Similarly, Gartner predicts that over the next two years, 45% of global organizations will be impacted in some way by a supply chain attack. The takeaway – your organization is only as strong as its weakest link.

The bad news does not end there. The same IBM report also found that 82% of breaches included cloud-based data, with ransomware at the forefront. More frighteningly, even with blockchain safeguards, hackers got away with more than $2 Billion in cryptocurrencies in 2023.

However, that would still just be some nominal pocket change in the burgeoning $8 Trillion cybercrime economy of 2023. To put this in perspective, the world lost $255,000 every second this year to cyberattacks.

According to Gartner, 63% of respondents report that their organization has experienced a supply chain attack in the past year.

Accounting for nearly 25% of all cyberattacks, the increasing adoption of robotics, IoT (Internet of Things) technology, and automation by the manufacturing industry has painted a bullseye for cybercriminals.

Out of the victims of ransomware, more than one-third of manufacturers paid the ransom to get their data back. However, only 1 in 4 companies were able to thwart the attacks before their data was fully encrypted.

Moreover, the adoption of AIML not only in storage but operations of digital assets daily, has increased the attack surface even more.

How can you protect your manufacturing firm from cyberattacks?

Implement access controls and limit privileges for employees.

Employ intrusion detection and prevention systems.

Regularly update and patch industrial control systems to address vulnerabilities.

Finance & Insurance

Key Takeaways

17.5 million credit card information was sold on the black market.

Hackers registered over 42,000 imposter domains to execute a large-scale phishing attack in 2023.

In Q1 2023, phishing attacks disproportionately targeted the finance sector, constituting a substantial 23.6% of total cyber incidents.

With a rise in politically motivated attacks, the financial sector has appeared as a favourite. Losses incurred by financial organizations amounted to approximately $5.9 million per incident in 2023.

According to Security Boulevard, 80% of the organizations met at least one breach related to weak authentication.

The impacts of these cyberattacks are massive, as evident from the Transit Finance incident where $29 Million was stolen by a hacker. Additionally, 71 percent of organizations were victims of payment fraud attacks or attempts.

How can you protect your financial firm from cyberattacks?

Strengthen cybersecurity with encryption and regular updates.

Develop an agile incident response plan.

Leverage advanced threat detection for real-time monitoring.

Consumer Businesses

Key Takeaways

In retail, the average cost of a data breach in 2022 was $3.28 million.

Fifty percent of retail cyberattack victims were extorted, and 25% had their credentials harvested.

More than 20% of customers stop buying from companies that have been hacked.

Living in a post-pandemic world with remote operational models, the digitization trend has become a necessity for E-commerce businesses. Sixty-eight percent of companies experienced a targeted attack on their networks and suffered data loss as a direct result.

Sixty-three percent of such data breaches come from exploiting internal weak points in a company’s customer and vendor network. Moreover, according to recent research by BDO, thirty-four% of retailers said that cyber-attacks or privacy breaches were their most serious digital threat.

As such, in 2023, E-commerce fraud cost the retail sector more than $48 billion globally.

How can you protect your consumer business from cyberattacks?

Use secure and compliant payment processing solutions.

Regularly analyze network activity for anomalies and potential security threats.

Develop and test a clear incident response plan to efficiently handle breaches.

Education

Key Takeaways

In 2023, over 700,000 threats were detected between April and June alone.

In 2023, the rate of ransomware attacks in the education sector was more than double at 44% of the rate reported in 2021.

The average cost of data recovery dropped from $1.42 million in 2022 to about $1 million in 2023.

The education sector, with its extensive sensitive data and limited cybersecurity resources, has been an appealing target for cybercriminals for the past few years. With an average of almost 2,000 attacks per organization reported weekly in 2022, the education industry has had it rough.

To put the above in perspective, of the above attacks, 36% were attributed to compromised credentials and 29% to exploited vulnerabilities, all of which could have been prevented by simple MFA.

According to IBM, the average cost of a data breach in the higher education and training sector was $3.7 million in 2023, down from $3.9 million in 2022.

Healthcare

Key Takeaways

According to the U.S. government's OCR, healthcare firms reported 145 data breaches in the first quarter of 2023 alone.

Phishing attacks were used in 45% of all healthcare data breaches in 2023.

Ransomware attacks have been a major threat to healthcare organizations, with 707 attacks in 2023.

Compared to the previous year, the number of cybersecurity breaches has increased, however, the loss from each incident has risen significantly.

Simply put, the number of individuals affected by such breaches jumped from thirty-one million in the second half of 2022 to a new record of forty million in 2023. Furthermore, third-party data breaches have also had severe consequences.

More than 119 pediatric practices and 2.2 million patients were affected by a single incident.

Furthermore, New York-Presbyterian (NYP) Hospital reported a data breach that affected approximately 12,000 people in September 2022.

Similarly, Aveanna Healthcare was hit with several phishing-related data breaches, for which they agreed to pay $425,000 in settlements.

CYBERSECURITY IN QATAR

Cybersecurity in Qatar is characterized by a comprehensive and forward-thinking approach, aimed at protecting the nation's digital infrastructure, enhancing its cybersecurity capabilities, and ensuring a secure digital environment for its citizens and businesses. The country is positioning itself as a global leader in cybersecurity through the adoption of advanced laws, policies focused on technology and cybersecurity, and significant investments in cybersecurity infrastructure and talent.

A pivotal element in Qatar's cybersecurity framework is the establishment of the Qatar Computer Emergency Response Team (Q-CERT) in 2005, which plays a central role in monitoring online threats, ensuring the safety of the Internet for the citizens, and fostering international collaboration on cybersecurity issues. Additionally, the Qatar National Cyber Security Strategy (2024-2030) emphasizes the importance of implementing comprehensive measures to secure the nation's digital space, showcasing the government's commitment to maintaining and enhancing cybersecurity.

Qatar's legal framework for cybersecurity includes several key laws aimed at protecting personal data privacy, ensuring the security of critical information infrastructure, and fostering cooperation and information exchange both domestically and internationally. These laws are designed to safeguard sensitive information, protect critical sectors from cyber threats, and educate citizens and organizations on best cybersecurity practices.

Qatar's strategic initiatives in cybersecurity also involve collaborations with international partners and the cultivation of skilled cybersecurity professionals, underpinned by a strong regulatory and policy landscape. This multifaceted approach demonstrates Qatar's dedication to creating a robust cyber ecosystem, offering significant opportunities for investment and collaboration in the cybersecurity sector.

REFERENCES

https://www.checkpoint.com/cyber-hub/cyber-security/
https://www.careerride.com/view/charms-and-challenges-of-cyberworld-15787.aspx
https://www.zscaler.com/resources/security-terms-glossary/what-is-cybersecurity?
https://me-en.kaspersky.com/
https://www.ibm.com/blog/types-of-cyberthreats/
https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat/