IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security to Safeguard Cyber Attacks

RISHABH SHARMA

The Shri Ram School (Aravali), Gurgaon, Haryana, India

Abstract: A virtual world or an online world is referred to as cyberspace. It is a communication-enabled artificial world created by computers or internet-enabled devices or components. It is a web-based platform that allows users to interact and communicate with one another. Cybercrime is an area of crime that is rapidly expanding around the world. It is defined as an offense committed using computers or internet-enabled devices. Currently, most of the economic, social, and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations, and government institutions, are carried out in cyberspace. Recently, many private companies and government organizations worldwide have been facing the problem of cyber-attacks. With the increasing volume and sophistication of cyberattacks on data at both the personal and organizational levels, there is a greater need to safeguard personal information and sensitive business data. This study aims to comprehensively review the standard advances presented in the cyber security field and investigate the challenges and preventive measures for the proposed methods. Different types of new descendant attacks are considered in detail. The paper will discuss how cyber-attacks steal millions of rupees or dollars from digital wallets and how an individual or organization can save them from such attacks.

Keywords: Cyber-attacks, Cyber security, Digital adoption rate, Organizational models, Economic impact, Reputational loss.

Introduction

The world relies entirely on digital space for communication and interaction in the modern era, whether through social media, financial transactions, or mobile transactions. As a result of technological advancement, people are becoming increasingly reliant on the Internet. The Internet is widely used for many activities, making people's lives easier and more enjoyable. Every sector, including railways, academics, research, space, telecommunications, health, banking, airports, and social media, is entirely dominated by the Internet or internet-enabled devices. Every innovation or technology positively impacts people's lives but also has some negative consequences. Every day, we can see crime rates rising in all societies worldwide. Everyone's lives are engulfed in a struggle between those who commit heinous crimes and those who seek to curb, prevent, detect, or punish criminal activity and attempt to strike a balance between them. People spend most of their time on digital platforms for social interaction, debate, pleasure, or work. The growing reliance on the digital world for communication, socialization, financial transactions, entertainment, and business is causing concern and complexity. Cybercrimes are offenses or illegal activities that occur on or through one or more components or mediums of the Internet.

India's digital industry has grown unprecedentedly in the history of the world's economies. Over the last two decades, all sub-sectors of this industry have seen revenue growth (hardware products have seen less progress). This has fueled the Indian economy's growth. The rapid growth of the digital sector and the Indian government's liberalization policies, such as lowering trade barriers and eliminating import duties on technology products, have contributed to the industry's growth. The COVID-19 pandemic has swept the globe, wreaking havoc on economies. The Indian I.T. Industry is still showing signs of life and resilience in the face of this unprecedented tragedy.

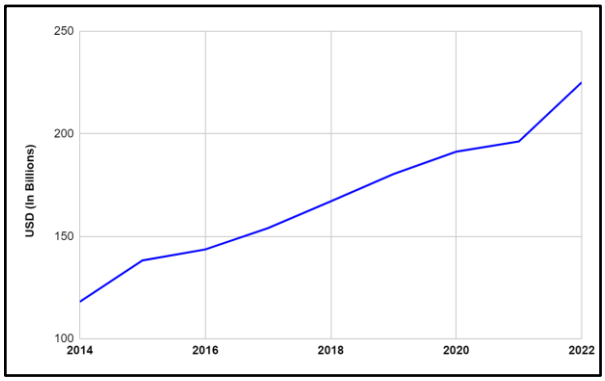

Fig 1: Market size of India's Digital market (In Billions of dollars)
© statista.com

India has the world's second-largest digital consumer base, growing at the second-fastest rate among major economies. India's inclusive digital model is bridging the digital divide and

bringing the benefits of technology to all population segments. New digital ecosystems in diverse sectors such as financial services, agriculture, healthcare, logistics, jobs, skills market, e-governance, and others could account for half of the potential economic value of $1 trillion in 2025.

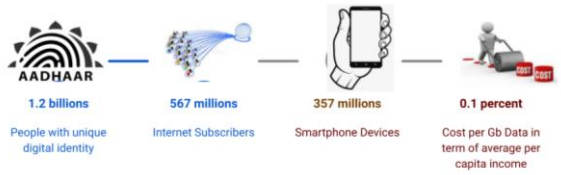

Fig 2: Key aspects of digital adoption
© McKinsey COVID-19 Digital Sentiment Survey

Women worldwide have less access to and benefit from technological advancements. The gender digital divide refers to this phenomenon. This disparity excludes women from political participation, healthcare, and education, exacerbating pre-existing social inequalities. Despite increasing internet access throughout the country, the digital divide on all three levels further disadvantages women in India. According to the PEW global survey, in 2021, 65% of men had access to the Internet compared to 35% of women in India, indicating that women lag in the country's digitalization.

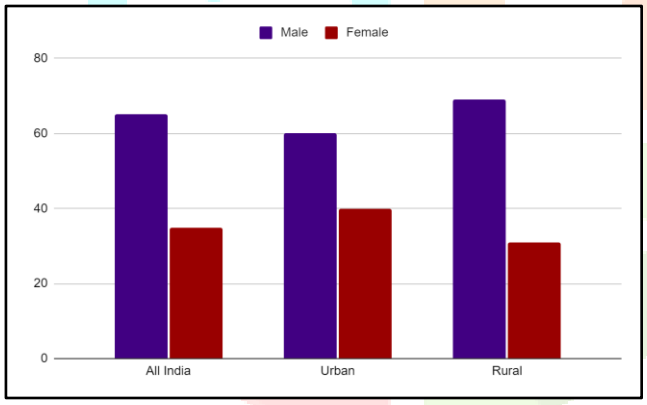

Fig 3: Gender digital adoption rate
© Telematics and Informatics

The world is more intricately linked than ever. In 1990, the total value of global goods, services, and finance flows was $5 trillion, or 24% of global GDP. There were approximately 435 million international tourist arrivals, and the public Internet was still in its infancy. In 2022, $38 trillion in goods, services, and finance were traded across borders, accounting for 41 percent of global GDP. International tourist arrivals have surpassed 1.36 billion. And the Internet has evolved into a worldwide network that instantly connects billions of people and countless businesses worldwide.

According to one study, cybercrime costs the global economy $470 billion in annual losses due to consumer data breaches, financial crimes, market manipulation, and intellectual property theft. Hackers can also endanger public safety and even national security. While businesses are frequently at the forefront of ensuring cybersecurity, governments can invest in research, share information, model good security practices, and develop thoughtful rules.

In India, cybercrime is defined as a voluntary and willful deletion that negatively impacts an individual's finances or computer system and is punishable under the I.T. Act 2000 (Information Technology Act) mentioned in the Indian Penal Code.

Current Scenario

According to reports, cybercrime accounted for 27.2% of Bengaluru's FIRs in 2019. The majority of Indians rely on YouTube for information, which is unauthenticated and unreliable. People have been concerned about online fraud, ATM pin leakage, and other issues, increasing their fear and slowing India's digitalization process. The Indian government, legislators, and executors have been attempting to reduce cyber crime in India for the past few years, but it has continued to rise. The majority of people are unaware of cybercrime, and they have become victims of it.

Most systems today rely on static passwords to authenticate users. Static passwords expose hackers, identity thieves, and fraudsters in this age of increased reliance on I.T. systems. Furthermore, hackers can use various techniques/attacks to steal passwords to gain access to their login accounts, such as guessing attacks, shoulder surfing attacks, dictionary attacks, brute force attacks, snooping attacks, social engineering attacks, etc. Many techniques and strategies for using passwords have been proposed, but many are difficult to use and practice. Two-factor authentications using OTP and ATM pin/cards have been implemented to solve the password problem in banking sectors and online transactions.

According to statistics presented in the parliament house, India has seen an increase in cyber security cases across the board (Government and aid organizations, Private sector organizations, and Individual level). Covid-19 has accelerated a trend that was already on the rise. The heavy reliance on technology that came with WFH becoming the norm worldwide was unavoidable. Furthermore, the increased adoption of 5G, device interconnectivity, new processes and procedures, updated employee profiles, and less-controlled work environments have increased vulnerabilities.

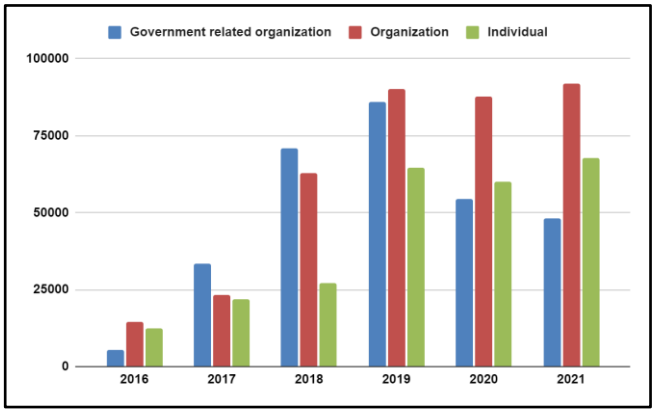

Fig 4: Number of cyber attacks reported in India
© National Crime Records Bureau

Cybercriminals use social engineering, phishing, identity theft, spam emails, malware, ransomware, and whaling to compromise their targets. According to the airline, hackers broke into Air India's servers and accessed the personal information of 4.5 million passengers. The Pimpri-Chinchwad Municipal Corporation's Smart City project in the Pune district, which Tech Mahindra manages, was attacked in March 2021.

Complete security is impossible to achieve, and cybersecurity comes at a cost. Businesses can expect to pay $3 to $5 per user per month for basic antivirus on their workstations and $5 to $8 per server per month for basic antivirus on their servers. Monitoring costs on average range from $100 to $500 per month for a small network to $500 to $2,000 per month for a medium-sized network. Most businesses should cost a quality e-mail protection service between $3 and $6 per user per month. Two-factor authentication can cost anywhere between $6 and $10 per user per month for your business. Hardware security keys cost between $30 and $60 for a one-time fee, depending on the manufacturer. A vulnerability assessment costs between $1,500 and $6,000 for a network with 1-3 servers and $5,000 to $10,000 for a network with 5-8 servers. Depending on the program's complexity, development can take anywhere from 5 to 20 hours. The hourly rate ranges from $149 to $479.

Recent Cyber attacks and breaches

In April 2022, Malwarebytes, a maker of anti-malware software, reported 280 cases of attacks by known types of ransomware. India was responsible for five of these attacks, or 2%.

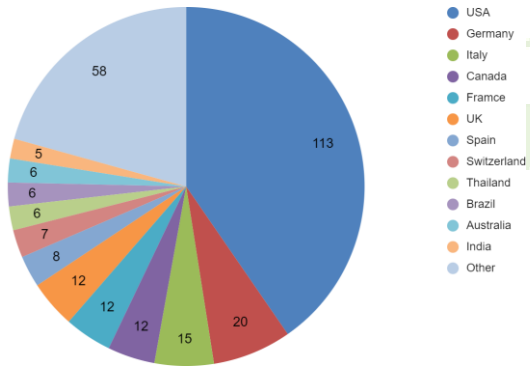

Fig 5: Cyber attacks reported across the globe in April'22
© Consultancy.in

SpiceJet successfully thwarted a ransomware attack that crippled the airline's systems and caused multiple flights to be delayed by several hours. While the incident resulted in frayed passenger tempers and tangled logistics at the very least, it has shifted the spotlight to the threat of ransomware attacks, which became more prominent in 2017. The fact is that cybercrime is not a problem unique to the aviation industry and must be addressed as a whole. We need a regulatory and policy environment that requires stricter security protocols across all industries.

Year	Cyber attacks & breaches
2022*	Razorpay, a Bengaluru-based fintech unicorn startup, has filed a complaint with cyber crime police alleging theft of 7.3 crores.
	The wedding planning and registry website Zola was hacked. A total of 0.1 percent of accounts were hacked, resulting in the theft of thousands of dollars from user accounts.
	Microsoft is no stranger to cyberattacks, and on March 20th, 2022, the company was targeted by a hacking collective known as Lapsus$.
	More than 500,000 records were compromised due to an attack on a third-party contractor, including documents classified as "highly vulnerable" by the Red Cross.
	Ronin is a blockchain gaming platform that uses cryptocurrency, so it's bound to be targeted by astute criminals – exactly what happened between November 2021 and March 2022.
	Plenty of hackers are motivated by politics rather than pure financial gain, and GiveSendGo's breach in February 2022 is no exception.

Table 1: Recent Cyber Attacks across the globe

To protect critical business assets, companies employ various sophisticated technologies and techniques. However, trust is the most crucial aspect of any cybersecurity program. All executive decisions about tools, talent, and processes are based on it. However, based on our observations, many organizations' cybersecurity initiatives lack trust due to competing agendas.

For example, senior business leaders and the board of directors may prioritize cybersecurity, but every employee must understand cybersecurity and follow Management's recommendations.

Types of Cybercrime

A.Crime against persons

(1) Assault by Threat – threatening a person's life or the lives of their families or those whose safety they are responsible for (such as employees or communities) via a computer network such as email, videos, or phones.

(2) Child pornography uses computer networks to create, distribute, or access materials that sexually exploit minors.

(3) Cyber laundering – the electronic transfer of illegally obtained funds to conceal the source and possibly the destination.

(4) Cyberstalking – using computer technology such as email, phones, text messages, webcams, websites, or videos to make explicit or implied physical threats that instill fear.

(5) Cyber terrorism – premeditated, usually politically motivated violence perpetrated against civilians using or aided by computer technology.
(6) Cyber theft is using a computer to commit theft. Breaking, DNS cache poisoning, embezzlement, unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy are examples of illegal activities.
(7) Yahoo Attack: Also known as 419 because such offenders are punishable under Section 419 of the Indian penal code. It is distinguished by the use of e-mail addresses obtained from Internet access points through e-mail address harvesting applications (web spiders or e-mail extractors). These programs can automatically extract email addresses from web pages. Indian fraud letters combine the impersonation scam warning with a variation of an advance fee technique in which an e-mail from an Indian offers the recipient a percentage of a large sum of money that the author, a self-proclaimed government official, is attempting to siphon out of the country.
(8) The Salami Attack:
Salami attacks are flamboyant economic scams or breaches of confidentiality through extensive data gathering.

B.Crime against property

(1) Crimes Against Intellectual Property - Intellectual property is a collection of rights. Any illegal act that deprives the owner of all or part of his rights constitutes a crime. Software piracy, copyright infringement, trademark infringement, patent infringement, design, service mark infringement, and theft of computer source code are examples of IPR violations.
(2) Cyber Squatting - When two people claim ownership of the same domain name, either by claiming that they registered it first or by claiming the right to use it before the other, or by claiming that they used something similar. For example, www.yahoo.com and www.yaahoo.com are two similar domain names.
(3) Internet Time Thefts - Hacking is the term used to describe the theft of time on the internet. It is the unauthorized use of another person's paid Internet hours by a third party. Someone who gains access to another person's ISP user ID and password through hacking or illegal means uses it to access the Internet without the other person's knowledge. If your Internet time has to be recharged frequently, despite infrequent use, you may be dealing with time theft.

C.Cyber Crimes against Government

(1) Cyber Terrorism - Cyber terrorism is a major source of domestic and international concern. Terrorist attacks on the Internet commonly take the form of distributed denial of service attacks, hate websites and e-mails, attacks on sensitive computer networks, and so on. Cyber terrorism puts the nation's sovereignty and integrity in jeopardy.
(2) Cyber Warfare refers to malicious and snooping hacking for political gain. It is a type of information warfare that is sometimes compared to conventional warfare, though this comparison is debatable in terms of accuracy and political motivation.
(3) Distribution of pirated software - It refers to the distribution of pirated software from one computer to another to destroy government data and records.

The Economical Impact & Valuation

According to Kaspersky telemetry, when the world went into lockdown in March 2020, the total number of brute-force attacks against remote desktop protocol (RDP) increased by 197%, from 93.1 million in February to 277.4 million in March. In India, the number increased from 1.3 million in February 2020 to 3.3 million in March 2020. Monthly attacks never fell below 300 million from April 2020, reaching a new high of 409 million in November 2020. India had the highest number of attacks in July 2020, with 4.5 million.

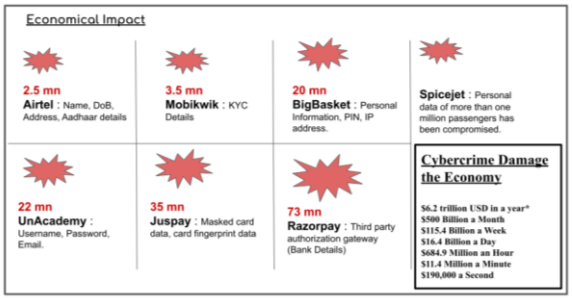

Fig 6: Economic loss reported due to cyber attacks
© Center For Strategic & International Studies

In India, data breaches have multiplied many times, regardless of the method used. However, the troubling trend in India has been firms' failure to acknowledge a breach, leaving individual users to wonder if their data is safe. If cybercrime were a country, it would be the world's third-largest economy after the United States and China, inflicting $6 trillion in global damages in 2021. According to an IBM Security study, the average total cost of a data breach in India will reach Rs 20 crore in 2022 (up 9.4% from last year), with the average time to contain a data breach increasing from 77 to 83 days. The cost of a single lost or stolen record is Rs 5,648, an 11% increase from 2020.

Over the past few years, Indian press & media has routinely broadcasted the story about the engagement of Intercountry cyber criminals. A Nigerian national involved in a fake job racket, allegedly victimizing at least 40 people, had recruited several women in his gang as money mules. Note that money mules in cybercrimes are often duped and recruited online to transfer stolen money illegally. The mules falsely think that they are employed in a legitimate business. The victims were asked to deposit Rs. 6,000–60,000 (US$ 110–1,100) as travel and related expenses for interviews. The women's bank accounts were used to receive the crime proceeds, and their ATM cards were used to withdraw cash. The victims were promised that the money would be refunded after the interview. In light of prior findings, which indicate a high degree of vulnerability of Indian women in cyberspace, this is yet another mode of victimization of women.

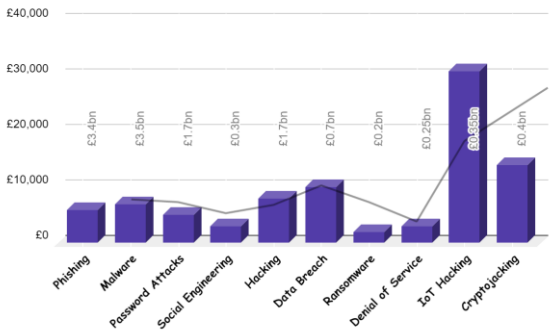

Fig 7: Economical impact of cybercrime
© Beaming & Opinium

According to the IT Governance website statistics, email is used to deliver 92% of malware. Mobile malware is rising, with the number of new mobile malware variants increasing by 71% in 2022. 99.9% of discovered mobile malware is found in third-party (Advertisement) app stores.

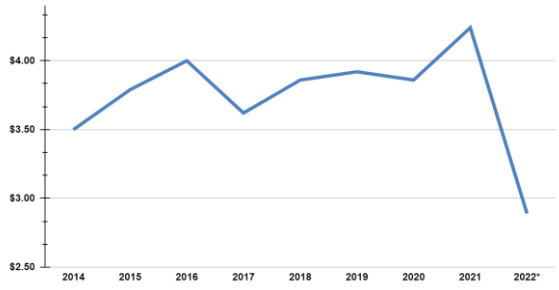

Fig 8: Global Average total cost of a data breach
© Forbes.com

Impact on organizations due to cyber attacks

Companies must recognize that cyber risk is a business risk in today's world." According to the report, IP theft accounts for at least 25% of the cost of cybercrime and poses a national security risk when it involves military technology. "IP theft and loss of opportunity are two areas of cyber crime impact that are extremely difficult to measure," said a business executive. "However, we have seen that IP theft and lost opportunities can be fatal for companies, particularly small and medium-sized businesses." According to a study, cyber attacks in India caused financial damages of USD 500,000 to Indian companies in the last 12-18 months.

A. ***Economic***: All types of attacks result in an organization's economic loss.
B. ***Reputational***: When a company suffers a cyber-attack, it loses people's trust and faith, making them hesitant to invest further in the company.
C. ***IP theft***: An organization's intellectual property, such as a patent, copyright, or trade secret, can be stolen, resulting in a significant loss.
D. ***Loss of sensitive business information***: Data with monetary value should be preserved, but its loss harms the organization because competitors can use it.
E. ***Lack of Trust***: When a company is subjected to a cyber-attack, customers lose faith in the company. It forces its clients to switch to other services.
F. ***Business Disruption/Lost Sales***: As a result of various attacks, businesses and sales are also impacted. Customers cannot access services due to a denial of service attack, resulting in a loss to the organization in a short period.
G. ***Equipment Loss:*** Malware can sometimes destroy networking equipment, requiring organizations to spend a significant amount of money to reinstall it.
H. ***Stock Prices***: Using malware, an attacker may interpret the stock prices of a company to lower the company's value and image.

Cyber-attacks have the potential to deliver economic blows, derail India's projected growth trajectory, and worsen relations with our neighbors, resulting in chaos.

Tech Support Scam

The scammers may represent as employees of a well-known technology company, such as Microsoft. They use a lot of technical jargon to convince you that your computer's problems are real. They may ask you to open some files or run a scan on your computer, only to tell you that the files or scan results indicate a problem when there is none.

The con artists may then

- Request that you grant them remote access to your computer, which will allow them to access all information stored on it as well as any network connected to it.
- Attempt to sign you up for worthless computer maintenance or warranty programme.
- Install malware that allows them to access your computer and sensitive data, such as user names and passwords.
- Request credit card information so that they can bill you for phoney services or free services available elsewhere.
- Try to sell you worthless software or repair services that are available for free elsewhere.
- You will be directed to websites where you will be asked to enter your credit card, bank account, and other personal information.

If a caller claims that your computer is having a problem, hang up. Even if the number is local or appears to be legitimate, an unexpected tech support call is a scam. Scammers use fake caller ID information to impersonate local businesses or well-known companies. If you suspect a virus or other threat, contact your security software provider directly, using the phone number listed on its website, sales receipt, or product packaging. Alternatively, seek the advice of a reputable security expert.

Recommendations

In the current era, organizations are handling security as a top priority, but they lack individual upskilling. Although they have introduced many learning programs, individuals consider it a question.

Although the number of cyber-attacks has increased over the last five years, organizations of all sizes are better at mitigating the risks. Many organizations correctly identified the malware as a top priority, with 45 percent reporting that they have taken additional security precautions to combat the threat, up from 26 percent in 2015. This will benefit organizations' faith if we create B2B and B2C models to secure the system and prevent such cyberattacks.

Many senior citizens in the United States live on fixed incomes, and they frequently want to increase the value of their estate and ensure they have enough funds to meet basic needs. Offenders in cyber scams persuade the elderly to invest in precious gems, real estate, annuities, or stocks and bonds by promising unrealistically high rates of return. Fake gemstones, uninhabitable property, or shares in a nonexistent or unprofitable company are common investments. Many seniors are computer savvy, but many more are not. Their computers are frequently not properly secured. Even if you have security software installed, it is critical that you set up automatic updates, activate a firewall, use a secure password, and so on. If you believe you cannot set up your computer security, it may be worthwhile to hire a computer technician from a reputable company to review the security settings and fix any problems you may have. As a result, basic computer skills are required for all individuals, particularly the elderly. Regular initiatives from government bodies are required to help them understand the usage and its complications. The context of the different categories below clearly explains the problem and how to avoid a data breach.

Social Media

Offenders use social media to commit crimes and find potential victims for burglaries. It is common on social media to post personal activities such as going on vacation or having dinner. Because these posts contain vital information about the victim, they become easy targets. Offenders seek easy targets because they have enough time to rob the victim's property. Telangana Today's leading example is the theft of 49 kilograms of gold jewelry from the victim's home. The victim posted details about the family trip on Facebook, including information such as the house being locked and burgled when he returned. According to the police, the person who committed the theft liked the post and took advantage of the opportunity to steal.

People tend to skip the content or simply accept it without reading the context, so it is critical to read and accept the user acceptance notice. Stopping social media threats requires education. People can educate themselves. However, businesses must implement training programs for all employees to detect and prevent social engineering and phishing. The first step is to educate users about the risks of disclosing too much information to the public online. Even private social media accounts could be used in an attack if the attacker gains access to private feeds. Users should never post private corporate information or information that could be used in an account takeover on their social media accounts.Other educational opportunities for employees include:

- Ad blockers should be used on corporate devices. If ad blockers are not an option, instruct employees to avoid clicking ads, particularly pop-ups that require users to download software to view content.
- Employees, even those in the same department, should not share passwords.
- Accept friend requests from unknown people, even if the user shares several friends.
- Avoid using social media sites while connected to public Wi-Fi hotspots. Man-in-the-middle (MitM) attacks are commonly used to snoop on data over public Wi-Fi.
- Passwords for user accounts should be changed regularly. However, users should be encouraged to change the passwords on their social media accounts.
- Secure your personal and private information. Social engineering cybercriminals can frequently obtain your personal information with only a few data points, so the less information you share publicly, the better. For example, if you post your pet's name or reveal your mother's maiden name, you may reveal the answers to two common security questions.

Education to All

While online learning provides numerous benefits for students and teachers, it is more important than ever to strengthen cybersecurity defenses to combat new and emerging threats. This proposal is intended to help teachers, parents, and students identify common cyber threats and provide tips on cybersecurity best practices to help you safely ease into the new school year.

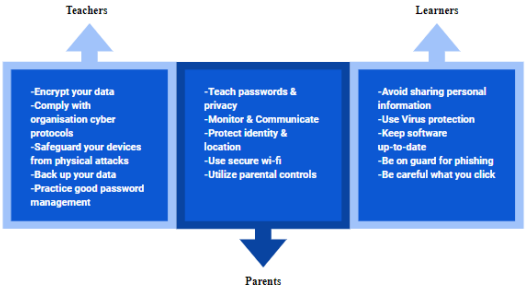

Fig 10: 5 things to remember for teachers, parents, and learners
© Unicef for every child

Teachers, parents, and students must arm themselves with the knowledge to protect their devices and personal information as cyber attackers continue to exploit gaps and introduce new threats and vulnerabilities.

One-Time Password(OTPs)

Although the organization has taken many initiatives and other important steps to reduce the thread, everyone must understand it and take preventive measures.

1. No financial institution will ever ask you to read your card details over the phone for verification or renewal. Never verbally give anyone your card number, CVV, or OTP. If your card information is compromised, your credit or savings account could be emptied.
2. Do not be tempted to click on SMSes from random numbers that look different or contain encrypted text with links. These have the potential to corrupt your phone. Use caution when clicking on links sent to you by unknown numbers. If you are asked to forward messages containing your OTP, refuse because an OTP is intended to secure your transactions. Giving it to someone else may assist them in diverting your transactions for their benefit.
3. Use a full-service internet security suite that provides real-time protection against existing and emerging malware, such as ransomware and viruses, and aids in the protection of your personal and financial information when you go online.
4. Antivirus installation, as the first layer of security, protects our files and folders from any cyber attack.

Information security is a broad topic. It includes both technical security and threats posed by users, whether due to general ignorance or naiveté when exposed to social engineering. IT professionals can install firewalls and antivirus software and enable regular updates of the operating system and antivirus software to improve technical security. However, no software exists to protect the system from its weakest link – the human. Parents can choose the appropriate software to improve the security of their child's computer or mobile phone. It should be noted. However, simple supervision is insufficient; a child should be appropriately educated about the dangers of the virtual environment and basic self-protection techniques.

Multi-Factor Authentication

Two-factor authentication is exactly what it sounds like: you need two factors to prove your identity rather than just one. Over the traditional username/password combination, two-factor authentication significantly increases security.

Fig 11: Two Factor Authentication

© International Journal of Latest Trends in Engineering and Technology (IJLTET)

Today, three universally recognized authentication factors exist:

- Something well-known: Examples include a password, a pin, a secret key, a private key, and so on.
- Something possessed: Examples include a debit card, credit card, smart card, passport, driver's license, identification card, and so on.
- Something inherent: examples of this Biometrics include fingerprints, face reorganization, and so on.

Use two-factor authentication whenever possible, as it is one of the most secure ways to protect access to your accounts and information.

The RSA SecurID authentication mechanism consists of a "token" that is assigned to a computer user and generates an authentication code at fixed intervals (usually 60 seconds) using a built-in clock and the card's factory-encoded random key (known as the "seed"). Each token's seed is unique and loaded into the RSA SecurID server (RSA Authentication Manager, formerly ACE/Server) as the tokens are purchased. Every 60 seconds, the RSA token generates a random code. This code is used to gain authentication for access to an account or server and the RSA PIN you choose. The RSA token has a two-factor authentication system, which includes:

- 'Something you know' – a four-digit PIN that has been memorized.
- The physical token generates a 6- or 8-digit code every 60 seconds.

RSA-based authentication is the same as two-factor authentication, but this service is commonly used at the organizational level rather than individually.

Conclusion

Preliminary research revealed that all target groups require additional education about the dangers of cybercrime and the importance of information security. To successfully address the issue of cybercrime, successful preventive techniques must be implemented in all target groups. As a result, we concluded that continuous education plays an important role in increasing user awareness and encouraging them to use preventive techniques in their daily lives. Following the completion of each educational module, an evaluation will be performed to assess the effects of the educational module implementation. An interdisciplinary conceptual framework is proposed to combine behavioral cybersecurity, human factors, modeling, and simulation. Enterprises should be involved in research to ensure that models function as intended. We will take the first step toward creating an information security culture by implementing these educational modules aimed at the youngest Internet users. It is proposed and recommended that individuals use two-factor authentication and organizations adopt RSA-based authentication to minimize the threat in the digital world. We can save data, billions of dollars, and the economy by implementing the proposed mechanism.

References

[1] Addae JH, Sun X, Towey D, Radenkovic M Exploring user behavioral data for adaptive cybersecurity. User Model User-Adap Inter 29(3):701–750. https:// doi.org/10.1007/s11257-019-09236-5

[2] Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? 11.

[3] Benson, M. L., Tamara D. M & John E. E. (2009). White-collar crime from an opportunity perspective. In S. S. Simpson & D. Weisburd (Eds.) The criminology of white-collar crime(pp 175–193). Heidelburg: Springer International Publishing.

[4] Bishop M. (2005). "Psychological acceptability revisited." In: Cranor and Garfinkel (Eds), Security and Usability, O'Reilly, pp.1-11 [chapter 1].

[5] Boulton, C. (2017, April 19). Humans are (still) the weakest cybersecurity link. https://www.cio.com/article/3191088/humans-are-still-the-weakest-cybersecuritylink.html

[6] Brostoff, S. and Sasse. M.A. (2000). "Are Passfaces more usable than passwords? A field trial investigation." In McDonald S et al (Eds): 'People and Computers XIV - Usability or Else', Proceedings of HCI, Sunderland, UK, pp.405-424, Springer.

[7] Carretero-Gomez, S., Vuorikari, R., & Punie, Y. (2017, April 28). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use https://ec.europa.eu/jrc/en/publication/eurscientific-and-technical-researchreports/digcomp-21-digital-competenceframework-citizens-eight-proficiency-levelsand-examples-use

[8] Cranor, L. and Garfinkel, S. (2005) Security and Usability: Designing Secure Systems That People Can Use. O'Reilly Media, Inc.

[9] Gregoric, U., 2010. Socialni inženiring v spletnih socialnih omrežjih. Available online: http://www.fvv.unimb.si/dv2010/zbornik/informacijska_varnost/gregoric.pdf

[10] Landauer, T.K., (1988). "Research methods in Human Computer Interaction." In Helander, M. (Ed.), Handbook of Human Computer Interaction, Amsterdam: NorthHolland, pp. 905-928.

[11] Murdoch, S., Drimer, S., Anderson, R. and Bond, M. (2010). "Chip and PIN is Broken". 2010 IEEE Symposium on Security and Privacy. doi: 10.1109/SP.2010.33.

[12] Maimon D, Louderback ER (2019) Cyber-Dependent Crimes: An Interdisciplinary Review. Ann Rev Criminol 2(1):191–216. https://doi.org/10. 1146/annurev-criminol-032317-092057

[13] On the (In)Security of Mobile Two-Factor Authentication Alexandra Dmitrienko2, Christopher Liebchen1, Christian Rossow3, and Ahmad-Reza Sadeghi1,1 CASED/Technische University at Darmstadt, Germany,2 CASED/Fraunhofer SIT Darmstadt, Germany,3 Vrije University Amsterdam, The Netherlands.

[14] Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., … Seamons, K. (2016). "We'Re on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 4298–4308. https://doi.org/10.1145/2858036.2858400

[15] Schjolberg, S. Lan, T., Xin, Z., Raduege, H., Grigoriev, D., Duggal, P. and (2008). Global Cyber Deterrence, views from China, the US, Russia, India and Norway, New York: The East West Institute

[16] 2014 SCC Online WIPO 506 Beach Body, LLC v. Cornel Ungureanu /Cyberland LLC World Intellectual Property Organization WIPO, Case No. D2014-0361.