Vol. 13. Issue.2. 2025 (April-June)
©KY PUBLICATIONS

http://www.bomsr.com
Email:editorbomsr@gmail.com

RESEARCH ARTICLE

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH

A Peer Reviewed International Research Journal

INTERNATIONAL STANDARD SERIAL NUMBER 2348-0580

A Relative Study on Cyber Security - Knowledge, Awareness and Threats

Meenu Goel[1], Kalpana Yadav[2]
[1]Assistant Professor, Department of Statistics, Mata Sundri College for Women, University of Delhi
E-mail: meenugoel@ms.du.ac.in
[2]Assistant Professor, Department of Statistics, Sri Venkateswara College, University of Delhi
E-mails: kalpana22yadav@gmail.com

DOI:10.33329/bomsr.13.2.55


Meenu Goel


Kalpana Yadav

Article Info
Article Received: 20/05/2025
Article Accepted: 24/06/2025
Published online: 30/06/2025

Abstract

The advent of the 21st century has been paralleled with ambitious strides for humankind, specifically in the areas of technology and computer innovation. Unfortunately, this quick-paced progression is pursued to the detriment of security and privacy in the virtual sphere. While lowered inhibitions around cyber security might account to be a necessity that is further catalysed by the global pandemic, the outcomes of the recent quick-changing mechanisms across industries and organizations can prove to be of momentous concern.

This article provides an attempt to investigate the underlying effects and correlation between these varying cyber threats and demographic factors such as age and gender. Research has also been carried out to study the degree of awareness and extent of faith in remedies and preventive measures placed by a sample of about 173 respondents of diverse backgrounds from the general population.

The findings of this study point to the need for increased cyber security awareness programs across demographic variation and enhanced policy and strategy framework.

Furnishing scope for the requisite trade-off between cyber safety and efficiency, this article hints at several areas and topics requiring special attention from policy makers as well as individual and organizational stakeholders.

Keywords: Cyber security, cyber bullying, malware, cyber safety, phishing, cyber security awareness. .

1. Introduction

The inception of the SARS-COV-2 pandemic has further accelerated human dependency on online systems. A recent McKinsey survey not only gives credence to this belief but takes a step further to affirm that these digital transformations have the potential to extend far beyond the scope and time frame of the immediate pandemic. This dramatic leap is causing sudden and drastic shifts in the routine functioning of several industries, most notably the healthcare and financial services industry. Undoubtedly, this interrelation is proving to be increasingly calamitous for the stakeholders and the participants involved. A report 'The Hidden Costs of Cybercrime' by Malekos Smith and Eugenia Lostri [13] estimates worldwide losses by virtue of cybercrime to claim over $1 trillion of the global economy annually. The study intends to find the public consciousness and understanding of these common cyber security threats plaguing and decelerating digital transformations. Some of these are listed below:

Malware attacks: An umbrella term for the representation of malicious software such as viruses, worms, Trojan horses, spyware, adware, among others. The earliest known malware was the 1971 Creeper which detected how a program moved between computer [14]. As time evolved so did these malwares and their functions. In 1974, a virus called Wabbit was discovered that copied itself so many times on a computer that it slowed down the system's performance to the point where it failed. The most popular of the earlier known malwares was the PC-Write TROJAN detected in 1986 that erased all the user's files. As computer system grew more complex, malwares not only affected at an individual level but also at a corporate level. Malwares rose dramatically as we entered the 21st century in terms of speed as well as what they infected and how far they reached due to internet access. There were malwares that leaked information from government sites. The innovation of crypto currency also invited the discovery of ransomware. Ransomware is a virus that threatens to publish or prevent access to a person's sensitive information unless a large sum of money is paid. A number of Anti-malware software have been developed to combat the ever-increasing number of malwares that exist nowadays.

Phishing: Cyberattacks that attempt to deceive users into disclosing confidential personal data like credit card information by virtue of social mechanisms. These may or may not include the use of malicious software. Phishing is usually done over email, phone or text where the person who attempts phishing impersonates someone. The most common consequences of phishing are identity theft or financial loss [15]. Identity theft is one of the fastest growing crimes in well-developed countries. For example; in America, identity theft usually occurs when a person's social security number is revealed. It is supposed to be kept confidential and not revealed to anyone until authorized by law. People pretending to be from

IRS (Internal Revenue Service) usually call victims and make it so that victims are forced to reveal their SSN due to dire circumstances. Well over 49 million people were victims of identity theft in 2025.

Common Features of Phishing Emails:

1. Unbelievable: It usually includes offers that seem extra-ordinary.
2. Very Small Time Gap: A person is required to revert back as soon as possible.
3. Unreliable Links and Attachments
4. Unrecognizable Sender

Phishing can be prevented by using spam filters in your emails which are specialized enough to recognize senders, software used to send the email or even block these emails. Web browsers nowadays usually come with a built-in feature that prevents access to unreliable sites. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) are used to determine whether the sender is human or a computer. Links in emails are secured by having a SSL (Secure Socket Layer) certificate.

Distributed-Denial-of-Service (DDoS) Attack: This form of cyber threat refers to attacks that attempt to overwhelm a website's server by directing repeated requests. These attacks could be motivated by several reasons including financial gains, moral conflicts, vengeance, etc. The very first DDoS attack was launched in 2000 to hack into a number of university websites and crash their websites [16]. In 2016, colossal DDoS attack took down websites of major companies like Netflix, Paypal, Github etc. Symptoms of DDoS attacks include: slow and limited access to websites and files, interrupted internet connection and excessive spam emails. The easiest way to protect yourself against DDoS attacks is the make sure you have a strengthened firewall. A firewall is device that secures your network by monitoring and filtering incoming and outgoing traffic [17]. AI is also used to detect DDoS attacks.

DNS Tunneling: Attacks to a website through encrypted messages sent via the Domain Name System. These threats can steal information as well as act as control centres for malicious software. DNS Tunneling is usually done by bypassing the firewall where malwares are sent to the DNS server and are allowed to get through the security scans [18]. Like every other malicious cyberattack one can protect themselves from DNS tunnelling by not clicking on suspicious link and keep tracks on domain names.

Other threats encompassing the scope of the study include Zero-day exploit, SQL injection, Man-in-the-middle attacks, and cyber bullying.

Zero-day exploit: Zero-day refers to the day when a particular software or system is launched. A zero-day exploit is done on the day, the product is launched where the attacker is aware of the vulnerability in the product but the vendor is not [19].

SQL injection: It is one of the most common ways of web-hacking where a code is written into the coding of the website, thereby destroying the database [20].

Man-in-the-middle attack occurs when an attacker assumes a position between a user and an application and actively eavesdrops or impersonates the user. This attack is used to steal personal information and credentials [21].

Cyber bullying is exploitative in nature. It materializes when a person uses internet platforms and social media to bully the victim online. Physical violence can be a by-product of cyber bullying and vice versa [22].

Moreover, in order to effectively understand the social and psychosomatic factors related to cyberthreats, it is imperative to discuss the faith placed by the general public in the law-and-order system concerning cyber delinquents and victims. Enhanced trust in law enforcement should discourage common cybercrimes and ensure a safe outlook for all involved. On the other hand, if more people feel the need for the implementation of new and improved cyber security policies and laws, this might point to an inefficient national cyber strategy.

Gupta and Agarwal (2018) noted that the rationale behind these threats could be varied, including fraud/illegal gain, greed, harassment, prank, etc. It has also been noted that there exists a significant correlation between many of these motives, some of the highest recorded between illegal gain/fraud and harassment (correlation of 0.83) and illegal gain/fraud and prank/satisfaction (0.76). It is also generally accepted that since illiteracy can be ruled out as a contributor to these crimes, the heavy focus should be placed on increasing levels of awareness about the implications and seriousness of the same among the literate and tech-savvy population.

Multiple research studies such as those conducted by Arifin et. al. (2019), Aljohani and Elfadil (2020), Chandarman and Niekerk (2020), Garba et.al. (2020) and Ahmed et. al. (2021), in various higher educational institutions have voiced the necessity for preparation programs, especially among the younger generation, to more effectively shed light on methods to improve safety in online systems as well as to enhance awareness of the consequences of committing grave cyber offenses.

Zwilling et. al. (2020) pointed that a significant portion of the respondents did not practice the requisite measures to ensure cyber security. Alharbi and Tassaddiq (2021) reemphasized that sufficient knowledge of cyber threats and security measures does not ensure the actual usage of these methods. Kenneth Olmstead and Aaron Smith [23] found that education plays a more significant role in an individual's awareness and knowledge of key cyber security questions than their age. Moreover, the authors also found that the number of people who were unsure of their answers was significantly more than those who gave incorrect answers. Apart from imparting knowledge about cyber security, there is also a need to curb and counter the misinformation and myths about these issues.

Overall, it was found that awareness about cyber security heavily depended on the topic at hand as well as the technological depth involved. In fact, out of over 1000 surveyed people, only 1% could answer all the cyber security-related questions that were asked.

Harknett and Stever (2011) listed the 2009-10 Government Accountability Office (GAO) Recommendations for cyber security and their subsequent state of progress the following year. The authors believe that their findings point to the necessity of a study national strategy for these issues. Moore (2010) points to the economic challenges, a seldom overlooked factor, as a major hindrance concerning cyber security issues. It has also been argued that economies suffer from a trade-off between cyber security and efficiency, which could help explain not

only why the optimal state of cyber security cannot be achieved, but also why it might be undesirable. For instance, although offline transactions cannot be plagued by cyber threats and thus, help prevent huge economic losses, they might not always be preferred keeping in mind the convenience of the user. However, the problem in this trade-off framework arises when those responsible for the decision-making processes in setting the balance between cyber security and efficiency do not necessarily suffer from its consequences, i.e., the problem of misaligned incentives.

Discussing cyber security issues in the present-day context, Williams et. al. (2020) advocated for the increased need to implement cyber security practices in pandemic events such as the SARS-COV-2. This is heavily attributed to the enhanced dependency on online systems during these times. Some specific sectors such as the healthcare industry can become extremely vulnerable to these attacks, and it is thus the need of the hour to focus on cyber security issues and awareness, both among the general population as well as in the context of large companies and organizations.

2. Objective of the study

The objective of this article is to identify the level of cyber security knowledge and to focus on the awareness and attitudes of people toward multiple cyber security threats, like viruses, phishing, cyber bullying, data breaches, etc.

3. Research Methodology

The survey technique was used to attain the objectives of the study. The survey was conducted online to obtain a large sample of people of different age group in an efficient and ethical manner. The questionnaire consisted of 25 questions to cover different aspects of cyber security, including demographics; internet usage; cyber bullying; the use of security tools, such as anti-virus and firewall; phishing awareness; cyber safety and cyber security knowledge. The survey took one month before it was disabled, a total of 173 valid responders have filled the survey. So, a total of 173 responses was used for this analysis. Tableau and SPSS were used in analysis plans and to produce results in this study.

4. Data Analysis and Interpretation

Demographics

From Table1 we can see that out of 173 responses female participants are the majority 61.3% with compared to male participants 38.7%. Most of the respondents lie in the category of 18 to 25 years of age with 84.9%, followed by 6.9% respondents of below 18 years of age. The rest of the participants are in the age-groups: 26-44 (5.2%) and above 45 (2.9%). The education qualification level of the responders was classified in four categories and it was found that the majority of them were 12^{th} pass i.e., 44.5%, 33.5% responders were graduate, 11.6% responders were post-graduates, and 2.3% had higher degree (PhD or MBA). People from different professions had participated in this survey. The majority of responders were students 74.6%, followed by people in private job (19.7%), 2.9% were in some business and 1.7% were in other occupations.

Table 1

Profile	Categories	Frequency	Percentage
Gender	Female	106	61.3
	Male	67	38.7
Age	Below 18	12	6.9
	18 – 25	147	84.97
	26 – 44	9	5.2
	45+	5	2.9
Qualification	10th pass	14	8.1
	12th pass	77	44.5
	Graduate	58	33.5
	Post-graduate	20	11.6
	Others	4	2.3
Occupation	Student	129	74.6
	Private Job	34	19.7
	Business	5	2.9
	Government Services	2	1.2
	Others	3	1.7

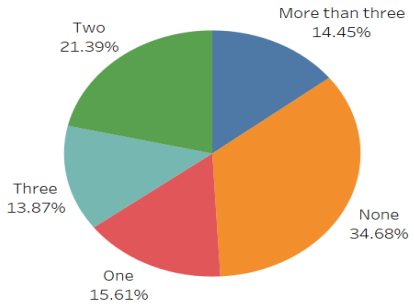

Figure 1: Percentage of people facing cyber-attacks

Figure1 shows the number of times responders have been victim of cyber-attacks. 15.61% responders have been victim of cyber-attacks only once, 21.39% responders have been victim of cyber-attacks twice,13.87% responders have been victim of cyber-attacks thrice while 14.45% responders have been victim of cyber-attacks for more than three times. 34.68% responders have never been victim of cyber-attacks.

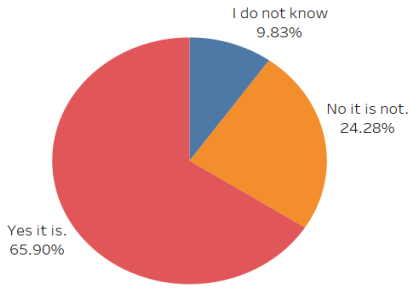

Figure 2: Installation of antivirus

Figure 2 shows that 65.9% responders have antivirus installed in their systems, 24.28% responders do not have antivirus installed in their systems while 9.83% do not even know if antivirus is installed or not.

Out of those who have antivirus installed in their systems, 45.7% claims that antivirus get updated automatically on their systems,15.6% update it occasionally, 3.5% update it at least once in a month, 4.6% update it at least once in a week, 2.3% update it at least twice in a week, 14.5% never update it while 13.9% have never updated it after the subscription expired.

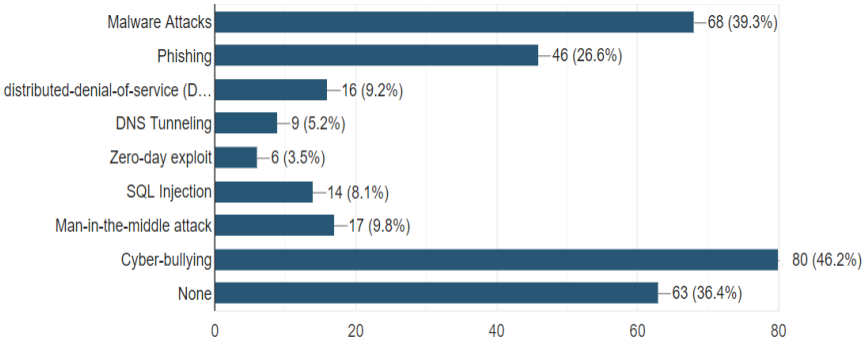

Figure 3: Cyber security Knowledge

Figure 3 shows that 46.2% responders have knowledge about cyber bullying, 39.3% have knowledge about malware attacks, 26.6% have knowledge about phishing, 9.8% know about man-in-the-middle attack, 9.2% know about distributed-denial-of-services (DDoS) attack,8.1% know SQL injection, 5.2% have knowledge about DNS tunnelling, 3.5% know about zero-day exploit while 36.4% responders do not have knowledge about any of the terms mentioned above.

5. Hypothesis Testing:

Test 1:

H_0: There is no significant difference in cyber security knowledge with male and female.

H_1: There is significant difference in cyber security knowledge with male and female.

Table 2: Group Statistics

Group Statistics for Cybersecurity Awareness

	Gender	**N**	**Mean**	**Std. Deviation**	**Std. Error Mean**
Do you have sufficient information about cyber security and its roles?	Male	67	1.9254	.84052	.10269
	Female	106	2.1038	.80391	.07808

Table 3: Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	D.f.	Sig. (2-tailed)	Mean Difference	S..E Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Do you have sufficient information about cyber security and its roles?	Equal variances assumed	0.39	0.533	-1.397	171	0.164	-0.178	0.127	-0.43	0.073
	Equal variances not assumed			-1.383	135.8	0.169	-0.178	0.129	-0.433	0.076

Since the p – value is greater than 0.05 we accept the null hypothesis and reject alternative hypothesis i.e., there is no significant difference in cyber security knowledge with male and female.

Test 2:

H_0: There is no significant difference in cyber security awareness with male and female.

H_1: There is significant difference in cyber security awareness with male and female.

Table 4: Group Statistics

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Do you know how to tell if your computer is hacked or infected?	Male	67	1.60	.494	.060
	Female	106	1.60	.491	.048

Table 5: Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	T	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Do you know how to tell if your computer is hacked or infected?	Equal variances assumed	0.03	0.862	-0.088	171	0.93	-0.007	0.077	-0.158	0.145
	Equal variances not assumed			-0.088	139.927	0.93	-0.007	0.077	-0.159	0.145

Since the p – value is greater than 0.05 we accept the null hypothesis and reject alternative hypothesis i.e. there is no significant difference in cyber security awareness with male and female.

Test 3:

H_0: There is no association between cyber security knowledge and number of cyber bullying cases faced.

H_1: There is association between cyber security knowledge and number of cyber bullying cases faced.

Table 6: Chi-Square Tests

	Value	d.f.	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)
Pearson Chi-Square	16.576[a]	8	.035	.032
Likelihood Ratio	16.447	8	.036	.051
Fisher's Exact Test	15.718			.039

Since, some of the observations are less than 10 so Fisher's Exact Test is used instead of Pearson Chi-Square Test. Now p-value for Fisher's Exact Test in Table 6 is 0.039 which is smaller than 0.05, thus we reject H_0 and accept H_1, i.e., there is association between cyber security knowledge and number of cyber bullying cases faced.

Table 7: Symmetric Measures

		Value	Approximate Significance	Exact Significance
Nominal by Nominal	Phi	.310	.035	.032
	Cramer's V	.219	.035	.032

The value of Cramer's V in Table7 is 0.219 which shows that there is moderate association between the variables.

Test 4:

H_0: Gender will have no significant effect on cyber safety.

H_1: Gender will have significant effect on cyber safety.

H_0: Age will have no significant effect on cyber safety.

H_1: Age will have significant effect on cyber safety.

H_0: Gender and Age interaction will have no significant effect on cyber safety.

H_1: Gender and Age interaction will have significant effect on cyber safety.

Table 8: Tests of Between-Subjects Effects

Dependent Variable: Cyber safety

Source	**Type III Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Corrected Model	59.584[a]	7	8.512	2.33	.027
Intercept	1159.114	1	1159.114	317.17	.000
Gender	16.686	1	16.686	4.57	.034
Age	12.236	3	4.079	1.12	.344
Gender × Age	3.376	3	1.125	0.31	.820
Error	602.994	165	3.655		
Total	6135.000	173			
Corrected Total	662.578	172			

In Table 8, since the p-value of first factor, gender is 0.034 which is smaller than 0.05 so the first null hypothesis is rejected and alternative hypothesis is accepted i.e., gender will have significant effect on cyber safety. The p-value for second factor, age is 0.344 which is greater than 0.05 so the second null hypothesis is accepted i.e. age will have no significant effect on cyber safety. The p-value for the interaction of gender and age group is 0.820 which is again greater than 0.05 so the third null hypothesis is also accepted i.e., gender and age interaction will have no significant effect on cyber safety.

6. Limitations of the Study

The findings presented in this article provided important points for developing cyber security awareness program, but there are some limitations that needs to be highlighted. The questions of the survey should be checked by cyber security experts. Although the preliminary data produced valuable results but since the sample size was limited to 173 responders so the research needs to be carried out on bigger sample size to improve the findings.

7. Conclusion

Cybercrimes are one of the gravest threats to national security. Visiting the websites which are already infected with viruses, opening phishing e-mails, identity theft, online extortion, sharing confidential information over the phone, or exposing personal information on social media tend to the stealing of personal information of netizens.

In this study, we evaluated level of cyber security knowledge of people of various age groups, via online survey technique. Based on the survey results, it is concluded that people are not that much aware and hence knowledge should be promoted on multiple cyber security concerns, such as cyber-bullying, data breaches, vulnerabilities, attacks, and incidents, to help them strengthen their security position. Proper measures need to be taken to escalate the cyber awareness level amongst them. Fully fledged cyber awareness will help them in protecting themselves from crackers, therefore, the awareness has to be created at higher level

References

[1]. Ahmed, O. S., Nasef, S. A., Al Rawashdeh, A. Z., & Eltahir, M. E. (2021). Teacher's awareness to develop student cyber security: A case study. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(10), 5148–5156.

[2]. Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), 1–15. https://doi.org/10.3390/bdcc5020019

[3]. Aljohani, W., & Elfadil, N. (2020). Measuring cyber security awareness of students: A case study at Fahad Bin Sultan University. *International Journal of Computer Applications, 9*(6), 141–155.

[4]. Arifin, A., Mokhtar, U. A., Hood, Z., Tiun, S., & Jambari, D. A. (2019). Parental awareness on cyber threats using social media. *Malaysian Journal of Communication, 35*(2), 485–498.

[5]. Chandarman, R., & Niekerk, B. (2020). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication, 20*(20), 133–155.

[6]. Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe: A quantitative approach. *International Journal on Emerging Technologies, 11*(5), 41–49.

[7]. Gupta, D., & Agrawal, N. (2018). Empirical study of cyber crimes in India using data analytics. *Global Journal of Enterprise Information System, 10*(1), 99–103.

[8]. Harknett, J. R., & Stever, A. J. (2011). The new policy world of cybersecurity. *Public Administration Review, 71*(3), 455–460. https://doi.org/10.1111/j.1540-6210.2011.02367.x

[9]. Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

[10]. Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research, 22*(9), e23692. https://doi.org/10.2196/23692

[11]. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

[12]. The hidden costs of cybercrime. (2020). *McAfee & CSIS Report.* https://books.google.co.in/books/about/The_Hidden_Costs_of_Cybercrime.html?id=mG0jzgEACAAJ

[13]. A brief history of malware – Its evolution and impact. (2018). *Malware News.* https://malware.news/t/a-brief-history-of-malware-its-evolution-and-impact/19191

[14]. Phishing.org. (n.d.). What is phishing and what are the common features of phishing emails? Retrieved August 28, 2025, from https://www.phishing.org/what-is-phishing

[15]. Norton. (n.d.). DDoS: What is a distributed denial of service attack? Retrieved August 28, 2025, from https://us.norton.com/blog/emerging-threats/ddos-attacks

[16]. Check Point. (n.d.). What is a firewall? Retrieved August 28, 2025, from https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall

[17]. What is DNS tunneling and how it is prevented? (2022). *CISO MAG.* https://cisomag.com/what-is-dns-tunneling-and-how-is-it-prevented

[18]. Fortinet. (n.d.). What is a zero-day attack? Retrieved August 28, 2025, from https://www.fortinet.com/resources/cyberglossary/zero-day-attack

[19]. W3Schools. (n.d.). SQL injection. Retrieved August 28, 2025, from https://www.w3schools.com/sql/sql_injection.asp

[20]. Imperva. (n.d.). Man in the middle (MITM) attack. Retrieved August 28, 2025, from https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm

[21]. UNICEF. (n.d.). Cyberbullying: What is it and how to stop it. Retrieved August 28, 2025, from https://www.unicef.org/stories/how-to-stop-cyberbullying

[22]. Pew Research Center. (2017). What the public knows about cybersecurity. https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2017/03/PI_2017.03.22_Cybersecurity-Quiz_FINAL.pdf