Issues in Information Systems
Volume 26, Issue 2, pp. 361-372, 2025

DOI: https://doi.org/10.48009/2_iis_128

Generational perception of ransomware-as-a-service (raas) and attitudes toward ransomware payments

Prayaanshu Pradhan, *Washburn University, prayaanshu.pradhan@washburn.edu*
Kevin Ong, *Washburn University, kevin.ong@washburn.edu*
Utsav KC, *Washburn University, utsav.kc@washburn.edu*
Nan Sun, *Washburn University, nan.sun@washburn.edu*

Abstract

The purpose of this research is to determine whether there are generational differences in perceptions and attitudes towards Ransomware-as-a-Service (RaaS). RaaS is one of the growing cybersecurity threats. RaaS can enable individuals with no technical expertise to deploy ransomware attacks. We conducted a survey where participants from various age groups were asked about their views on ransomware, their willingness to pay ransoms in a cyberattack, and the factors influencing their decisions. The research aims to understand the motivation behind individuals who might think of using RaaS for financial or personal gain. The results of this study provide insights into how different generations perceive the risks of RaaS and can contribute to cybersecurity awareness and policy development.

Keywords: ransomware-as-a-service, generational difference, ransom payment, cybercrime perception, cyber risk behavior.

Introduction

In the digital age, data is an asset, ranging from personal photos and medical records to financial information and critical infrastructure systems. As society grows increasingly reliant on digital technologies, the risk of cyberattacks continues to rise. Cyber-attacks are not only becoming more frequent but also more sophisticated and damaging. The global cost of cybercrime is said to reach $13.82 trillion by 2028 (Moore, 2022). Among the different types of cyberattacks like Phishing and Malware, Ransomware has become one of the most dangerous and fast-growing cyber threat. Ransomware is a type of malware that encrypts a victim's data, with attackers demanding payment in exchange for restoring access. In the first half of the year 2022, there were nearly 236.7 million ransomware attacks worldwide and by 2031 ransomware is expected to cost victims around $265 billion (Palatty, 2025).

This threat is more dangerous with the help of Ransomware-as-a-Service (RaaS). RaaS allows users with little to no technical expertise to launch ransomware attacks by purchasing or renting pre-built ransomware kits from the dark web. These kits often come with user guides, support, and malware tools, can cost as little as $40 (Baker, 2023). With ransomware accessible to anyone it is important to examine generational perception, to help shape prevention strategies.

Understanding generational differences is important because each age group has different life experiences, digital skills, and financial situations. Older generations are usually more settled in their careers with more financial assets and greater need to protect their personal information, making them more cautious about cyber risks. Younger generations, while more tech-savvy, may downplay threats or take more online risks due to overconfidence. These differences suggests that perceptions of RaaS may differ by generation, so cybersecurity strategies need to consider these factors as well.

This study explores how individuals from different generations perceive and respond to ransomware and Ransomware as a Service. The research tries to identify generational differences in awareness, willingness to pay ransoms, and motivations for engaging with ransomware. The study addresses these research questions:

1. Do cross generations view RaaS differently?
2. Are there generational differences in attitudes toward paying ransoms in a ransomware attack? What factors influence willingness to pay a ransom in a RaaS attack? How much are they willing to pay to recover data after a ransomware attack?
3. What factors drive to invest in ransomware for personal gain? Are younger generations more likely to engage with RaaS for personal gain?

We believe our research contributes to the field of cybersecurity studies in several meaningful ways. First, it offers insights into the ethical attitudes, risk perceptions, and behavioral intentions of different age groups toward ransomware. Second, it provides empirical evidence on how awareness and willingness to pay vary across generations and identify key factors influencing these behaviors. Third, the study examines the motivations behind potential misuse of RaaS. Finally, our findings can inform the development of targeted cybersecurity training and awareness education that address generational gaps in understanding ransomware threats.

Literature Review

Ransomware has become one of the most violent cyber-attacks in recent years and the rise of Ransomware as a Service has also increased cybercrimes across the globe (Webroot, 2024). People can use RaaS as subscription-based where the criminals provide attackers with the tool kits and scripts for cyber-attacks and revenue-based sharing where attackers join forces and conduct the attack (Association, 2023). RaaS has lowered the barrier for these criminals which has increased the rise in this cyber-attack. Individuals and organizations reportedly have lost billions of dollars' worth of data due to ransomware attacks and have not shown any sign of a stopping point.

Due to RaaS, the attacker can infiltrate one's system within two days or less which shows how easy it is to infiltrate one's system. These attacks are destructive not just because of financial burden, but also loss of data and reputation of an individual or organization (Halcyon, 2024). As it keeps on growing, researchers have started to look at how different generations view these attacks and how willing they are to pay ransom. According to prior research, different generations view cyber threats differently with respect to awareness, risks, and responses to such attacks (Research, 2019). Different generations seemed to have different behaviors and attitudes toward ransomware attacks (Vonage, 2023). Baby Boomers, who are often less familiar with modern cyber threats, are particularly vulnerable to phishing and social engineering; they are more likely to report ransomware incidents to authorities rather than paying, with low willingness to pay due to distrust of digital payments and a preference for traditional recovery methods (Webroot, 2024). Generation X, while moderately tech-savvy sometimes underestimating risks, may consider paying if critical data is compromised, showing a medium willingness to pay depending on the volume of attack

(Webroot, 2024). Millennials, while more aware of cybersecurity risks, may still fall victim to them but tend to other explore alternatives like backups or decryption tools before paying, showing a low-to-medium willingness to pay and may prefer to negotiate before paying (Webroot, 2024). Generation Z, highly digitally literate but lacks real-world cybersecurity experience, they are more likely to ignore ransomware or attempt self-recovery, with very low willingness to pay as they rely on cloud backups or just ignore the threats (Webroot, 2024).

Previous studies have noted that there has been a difference in how much individuals pay and how much organizations pay (IBM, 2023). Most individuals cannot afford to pay a large amount of ransom, and some are unwilling to pay it too. On the other hand, big organizations pay millions of dollars' worth of ransom just to get their data back (IBM, 2023). Factors such as financial and psychological influence on how much people pay the ransom (Vonage, 2023). From a generational perspective, Baby boomers and Gen X may pay more ransom than Millennials and Gen Z, as they don't have much awareness of these cyber threats and most are not familiar with technologies so they cannot create backups, while millennials and Gen Z have better knowledge on technologies and probably create backups or find their own way to avoid paying ransom (Webroot, 2024).

Existing research emphasizes cybersecurity education (Fogel, 2009) and the implementation of multi-layered defenses, including regular backups and system updates to patch vulnerabilities (GlobalSign, 2023). However, while AI and machine learning are emerging as potential solutions (Security, 2024), their interaction with human factors remains understudied. Our research addresses this gap by analyzing threat response behaviors across different generations. Prior studies have largely overlooked behavioral influences on ransom payment decisions, particularly how generational differences shape victim responses. While some generational trends in cybersecurity awareness have been noted (Association, 2023), key assumptions—such as Baby Boomers' reluctance to pay ransoms—lack proper validation. Our study fills this gap by providing data-driven insights into generational differences in response to ransomware.

Methodology

Our research objective was to examine how different generations view Ransomware-as-a-Service and their attitudes towards paying ransom. We conducted a survey using Microsoft Forms. Before distributing the survey, we obtained approval from our Institutional Review Board (IRB) and conducted a pilot study to ensure that every question was clear and understandable by the participants. The survey was shared through various forms, including email, QR code, college clubs' local communities, workplace and in person recruitment in public areas. The data was collected mostly on our institution and our local community.

The survey was divided into four main sections. The first focused on demographics, collecting data on participants' age, gender, education level, occupation, number of computer science courses taken, and their confidence level in understanding ransomware. The demographics section helped group people by different generations and account for factors like education and tech experience that could affect the results. The questions were formatted as multiple choice for ease of analysis.

The second section assessed the participants' awareness and perception towards RaaS, based on the idea that knowledge about cybersecurity cab vary across generations. The section had a brief definition of ransomware and RaaS, followed by a Likert-scale questions (1-5) to measure agreement on statements regarding their familiarity with ransomware, generational differences in cybersecurity awareness, and personal vulnerability to ransomware attacks. Participants were also asked if they had ever encountered a ransomware attack or knew someone who were a victim of such attack.

The third section explored participants' willingness to pay a ransom in the case of an attack, based on ethical and psychological factors found in previous studies. We used a combination of Likert-scale, multiple choice and short answer questions to understand the factors that influence ransom payment decisions. We also asked participants how much they would be willing to pay and explored whether participants believed younger generation were more likely to pay, if paying encouraged cybercrime, and whether the government should intervene.

The final section focused on motivations for using ransomware, based on factors like financial stress, exposure to cyber-crime tools and perceived risks. Participants were asked to select potential reasons an individual might engage in RaaS. We also asked if they had seen RaaS advertisements, considered cybercrime for financial gain, or believed legal consequences were too weak to deter such activity. This section aimed on the socio-economic and psychological drivers behind cybercriminal behavior. These groupings ensured that each question served an analytical purpose in addressing the generational attitudes toward RaaS. After collecting the survey responses, we compiled the data in Microsoft Excel and began the preparation process. This included organizing the responses and standardizing formats to ensure compatibility with SPSS. Once the dataset was properly structured, we imported it into SPSS for analysis. Using SPSS, we performed descriptive statistics and group comparisons to identify trends and differences in generational differences in perception, attitudes and behaviors related to Ransomware-as-a-Service. This analysis helped us come to conclusions from the data and informed us of the findings presented in the results section.

Results

In this section, we report the survey results. The following tables present the analyzed survey data, including the mean and standard error for each question, rated on a 5-point scale from 'strongly disagree' to 'strongly agree'. The tables also show the mean difference between younger (age: 18 – 30) and older (age: 30+) generations and the corresponding p values. We received 124 complete responses. Most participants were male (58%), followed by females (40%) and those identifying as other (2%). The majority were between 18 and 30 years old (62%), while 38% were over 30. Most held some college education (32%) or a bachelor's degree (31%). Others had a high school diploma, associate's degree, or master's degree (10% each), a doctorate (6%), or graduate degree (2%). The largest group by occupation were students (34%), followed by people in education (19%) and various other fields (27%). Smaller groups worked in business/finance, healthcare (7% each), and IT/cybersecurity (6%). Over half of the participants (52%) hadn't taken any computer courses, while rest had taken between 1 to more than 10 courses.

Table 1 shows that most participants were moderately informed about ransomware, with 31% reporting a neutral level of awareness. About 24% were unconfident and 17% were completely unconfident, indicating that over 40% of respondents lacked confidence in their knowledge about ransomware. 22% were confident and only 6% reported being extremely confident in their understanding of ransomware, highlighting a general gap in cybersecurity awareness.

Table 1. Awareness level of Ransomware

Awareness Level	Percent
Completely Unconfident	17%
Unconfident	24%
Neutral	31%
Confident	22%
Extremely Confident	6%

Table 2 presents descriptive statistics on participants' perceptions and views of Ransomware as a Service. The highest mean response was for the statement "I believe that different generations perceive this threat differently" (mean = 4.19), while the lowest was for "I click on links that are unfamiliar". (mean = 1.81) indicating limited engagement in risky online behavior. Participants also showed moderate concerns about ransomware threats (mean = 3.68) and relatively low personal experience with ransomware attacks (mean = 1.90).

Table 2. Perception and views on RaaS

Statement	Mean (SE)
ConcernedThreat	3.68 (0.085)
KnowRaas	2.84 (0.126)
DiffGenPercieve	4.19 (0.069)
MyGenVuln	2.94 (0.102)
Training	3.20 (0.131)
ExpRansAttck	1.90 (0.086)
KnowSomeone	2.71 (0.113)
ClickLinks	1.81 (0.010)
YoungThanOld	3.90 (0.087)
MyGenAware	3.34 (0.092)

As seen in table 3, responses suggest mixed concerns of RaaS between generations. Participants aged 30 and older reported significantly higher concern about ransomware threats (ConcernedThreat, mean = 4.17) compared to younger generations (mean = 3.38), with a statistically significant mean difference ($p < 0.001$). Older generations reported significantly higher awareness that they knew about RaaS before taking the survey (KnowRaas, mean = 3.17) than the younger generation (mean = 2.64) and the difference is statistically significant ($p = 0.039$). Additionally, older individuals viewed their generations as more vulnerable to ransomware attacks (MyGenVuln, mean = 3.32) compared to the younger generation (mean = 2.70) with a statistically significant difference ($p = 0.003$). In contrast, younger individuals believe their generation is more aware of ransomware threats (MyGenAware, mean = 3.67) than the older individuals (mean = 2.81) with a statistically significant difference ($p < 0.001$). Results that show statistically significant differences are highlighted in Table 3.

Table 3. Generational Perception on RaaS

Statement	Mean (SE): Age 18-30	Mean (SE): Age 30+	Mean Difference	p-value
ConcernedThreat	**3.38 (0.108)**	**4.17 (0.107)**	**0.794**	**<0.001**
KnowRaas	**2.64 (0.157)**	**3.17 (0.202)**	**0.534**	**0.039**
DiffGenPercieve	4.21 (0.091)	4.17 (0.091)	0.038	0.794
MyGenVuln	**2.70 (0.118)**	**3.32 (0.172)**	**0.618**	**0.003**
Training	3.04 (0.165)	3.47 (0.210)	0.429	0.111
ExpRansAttck	1.92 (0.109)	1.85 (0.139)	0.071	0.689
KnowSomeone	2.60 (0.134)	2.89 (0.202)	0.296	0.206
ClickLinks	1.91 (0.134)	1.66 (0.153)	0.250	0.234
YoungThanOld	3.95 (0.101)	3.83 (0.159)	0.118	0.511
MyGenAware	**3.67 (0.102)**	**2.81 (0.145)**	**0.863**	**<0.001**

Table 4 represented results related to attitudes towards ransomware payments. Participants generally disagreed with the idea of paying ransom if they were attacked (PayRans, mean = 2.48), indicating they are reluctant to such action. When asked if paying ransom would encourage more cyber threats, respondents showed strong agreement (mean = 4.20). The participants were more neutral toward the idea of supporting critical infrastructure in the event of a ransomware attack (CriticalInfa, mean = 3.10). However, there was a strong agreement that government should be involved in ransomware incidents (GovInter, mean = 3.88).

Table 4. Attitude towards paying ransom

Statement	Mean (SE)
PayRans	2.48 (0.088)
PayEncAttack	4.20 (0.071)
CriticalInfa	3.10 (0.090)
GovInter	3.88 (0.087)
MyGenPays	2.85 (0.081)
MyGenValueMore	3.50 (0.078)

As seen in table 5, both generations generally disagreed with paying a ransom in a ransomware attack (PayRans), younger generation (mean = 2.60) were more likely to consider it than older generations (mean = 2.30), though this difference was not statistically significant. When asked if paying ransom would encourage more cyber-attacks, older generation agreed more (mean = 4.38) than the younger generation (mean = 4.09), and this difference was statistically significant ($p = 0.047$). Both age groups reported similar beliefs about their generation's likelihood to pay a ransom (MyGenPays, $p = 0.720$). However, the younger generation were more likely to believe that their generations places higher value on data (MyGenValueMore, mean = 3.67) compared to older generations (mean = 3.21) with a statistically significant difference ($p = 0.004$).

Table 5. Generational attitude towards paying ransom

Statement	Mean (SE): Age 18 – 30	Mean (SE): Age 30+	Mean Difference	p-value
PayRans	2.60 (0.107)	2.30 (0.152)	0.300	0.100
PayEncAttack	**4.09 (0.096)**	**4.38 (0.099)**	**0.292**	**0.047**
CriticalInfa	3.13 (0.113)	3.06 (0.150)	0.066	0.724
GovInter	3.83 (0.108)	3.96 (0.146)	0.126	0.483
MyGenPays	2.87 (0.103)	2.81 (0.131)	0.060	0.720
MyGenValueMore	**3.67 (0.790)**	**3.21 (0.907)**	**0.458**	**0.004**

Table 6 shows the distribution of participants willingness to pay the ransom to recover their important files if they were targeted in a cyber-attack. Almost half of the participants (46.0%, n = 57) said that they would not pay any ransom amount to recover their personal data. 26.6% of the participants were willing to pay less than $1000 and a small portion of the participants were willing to pay between $1,000 and $10,000. Only one participant was willing to pay more than $500,000. Additionally, 21.0% chose "It depends on the situation" when asked about paying the ransom.

Table 6. Willingness to pay ransom

Amount	Frequency (n)	Percent
$0 (I would not pay the ransom)	57	46.0%
<$1000	33	26.6%
$1000 - $10000	7	5.6
>$500000	1	0.8
It depends on the situation	26	21.0

Participants were also asked to select all the factors that would influence their decision to pay ransom if they were a victim of a cyber-attack. The most frequently selected factor was the value of data, followed by the likelihood of data recovery and law enforcement advice. Other influencing factors included: legal consideration, ransom amount, time sensitivity of data, and trust in attacker's promise to decrypt the data.

Overall, the value of data was the most influential while trusting the attacker to decrypt the data was the least influential among the options provided.

Table 7. Factors Influencing to pay ransom

FactorInfluencePayment	N	Percent	Percent of Cases
Value of data	84	28.0%	68.3%
Likelihood of data recovery	51	17.0%	41.5%
Legal consideration	42	14.0%	34.1%
Law enforcement advice	56	18.7%	45.5%
Ransom amount	31	10.3%	25.2%
Time sensitivity	23	7.7%	18.7%
Trust attacker to decrypt	13	4.3%	10.6%

Table 8 shows people's motivation to use RaaS. Most respondents strongly disagreed with the idea of personally considering engagement in RaaS (ConsiderRaaS, mean = 1.35) and did not agree to do so for entertainment purposes (RaaSForFun, mean =1.60).

However, participants agreed that younger generations are more likely to get involved in RaaS activity (YoungGenInvolv, mean = 3.56), and socio-economic pressure can be a contributing factor. Participants were nearly neutral on whether their own generation is likely to engage in such behavior (MyGenLessLikely, mean =2.98).

Table 8. Motivation toward using RaaS

Statement	Mean (SE)
ConsiderRaaS	1.35 (0.074)
YoungGenInvolv	3.56 (0.087)
RaaSAds	2.14 (0.096)
BuyRaaSEasy	3.13 (0.068)
SocioEcon	3.60 (0.073)
RaaSForFun	1.60 (0.083)
NoRisk	3.59 (0.086)
MyGenLessLikely	2.98 (0.095)

As shown in Table 9 responses to statements about motivation and accessibility of RaaS did not have many differences among the generations. Both younger and older generation strongly disagreed with considering involvement with RaaS. There was a statistically significant difference in agreement that socio-economic factors influence individuals' involvement with RaaS with younger generations agreeing more (mean = 3.74) compared to older generation (mean = 3.38, p = 0.017).

The younger generation were slightly more likely to agree that individuals may engage in RaaS for entertainment (RaaSForFun, mean = 1.71 vs 1.40), though the difference was not statistically significant (p = 0.068).

Table 9. Generational views on motivation on using RaaS

Statement	Mean (SE): Age 18 – 30	Mean (SE): Age 30+	Mean Difference	p-value
ConsiderRaaS	1.44 (0.099)	1.21 (1.09)	0.229	0.136
YoungGenInvolv	3.68 (0.102)	3.36 (0.153)	0.314	0.079
RaaSAds	2.13 (0.126)	2.15 (0.149)	0.019	0.924
BuyRaaSEasy	3.21 (0.089)	3.00 (0.101)	0.208	0.137
SocioEcon	3.74 (0.088)	3.38 (0.124)	0.357	0.017
RaaSForFun	1.71 (0.115)	1.40 (0.104)	0.310	0.068
NoRisk	3.66 (0.099)	3.47 (0.158)	0.194	0.273
MyGenLessLikely	2.64 (0.112)	3.53 (0.139)	0.887	<0.01

Discussion

The results of our study indicate clear generational differences in the perception of Ransomware-as-a-Service (RaaS). They offer valuable insights into how age influences attitudes toward cyber threats. These differences directly answer our first research question: Do cross generations view RaaS differently? The data suggests that while there is agreement that RaaS is perceived differently across generations (mean=4.19), older participants tend to view ransomware as a more severe cyber threat. Their higher concern levels (mean = 4.17 vs 3.38, p <0.001) and greater familiarity with RaaS (p=0.039) suggest that older generation might be more cautious of risks due to their experiences. This contrasts with the younger participants. Despite claiming greater awareness of ransomware threats, they were more prone to engage in risky online behavior, suggesting possible overconfidence of cyber threats in their generation.

Across generations, most participants were unwilling to pay ransom. Among them, 46% said that they would pay nothing and the mean agreement on paying ransom was overall low (2.48). However, younger generations showed a slightly higher willingness to pay (mean = 2.60 vs 2.30), though not significant. Older participants strongly believed that paying ransoms encourages cybercrime (p=0.047), suggesting a deeper ethical concern and possibly greater awareness of the implications of surrendering to attackers. Younger participants placing more value on personal digital content like photos and social media (p value = 0.004) further explains why they might be more inclined to consider paying the ransom.

The third research question focused on the factors that motivate engagement with RaaS. While most participants strongly rejected the idea of using RaaS for financial or entertainment purposes, the data reveals that younger individuals perceive themselves as more likely to engage in such activity (mean = 3.56). This suggests, even without explicit intent, younger people may acknowledge that economic or social conditions could push individuals toward illegal cyber activity. Socio-economic pressure was a strong motivator for the younger participants (p=0.017), highlighting the role of financial instability in shaping risky behavior.
The findings reveal an important generational divide. The older participants are more cautious and ethically driven, while younger participants are more confident but also more exposed and potentially vulnerable to the RaaS related opportunities. This difference underscores the urgent need for tailored cybersecurity education that goes beyond technical skills and includes ethics and awareness of social engineering tactics.

Implications and Recommendations

This research explored generational differences in perception of and attitudes toward Ransomware-as-a-Service (RaaS), including awareness levels, willingness to pay ransoms, and motivations behind

engagement in cybercrime. We found that older generations were more concerned but less confident in handling cyber threats, while younger participants were more tech-savvy but more likely to engage in risky behavior.

The findings suggest the need for age specific cybersecurity training. Practical and confidence building for older adults, and ethics and consequences focused for the younger generations. Public awareness campaigns should also address the ease of access to RaaS and emphasize the legal risks. Since the value of data and law enforcement advice heavily influenced ransom payment decisions, stronger public guidance and clear response protocols can help reduce ransom payments. Overall, education, policy and outreach must work together to lower the generational gaps and reduce the impact of ransomware.

Limitations and Future Research

Our study has several limitations. First, the sample size was small, which limits the generalizability of the findings. A larger sample would be preferred for a robust comparison and group analysis. Second, there is the gender imbalance. We had more male than female participants. In several cases where the survey has presented in person, female individuals often deferred participation to male counterparts, saying they lacked familiarity with technology and instead encouraged their husbands to complete the survey. Third, attempts to distribute surveys through flyers received limited engagement. Other means of data collection seemed to be more effective.

Lastly, while the research aimed to explore generational perceptions, the sample was composed of younger participants (18 – 30 years old), who made up to 62% of the total participants. This could affect the study's ability to fully capture the perspectives of older participants and limit the generalizability of age-based comparison. During outreach, participants aged 50 and above were hesitant to participate due to discomfort with technology or the digital survey format. Some agreed to scan the QR code and complete the survey later, but few followed through, making it difficult to gather responses from older generations.

Future research should aim for more balanced sample in terms of both gender and age. Alternative data collection methods and interviews may help engage older demographics and ensure their perspective are better represented. Comparing perceptions across different professional sectors, such as healthcare, education, IT and finance could highlight industry specific concerns. Additionally, individuals can explore how media exposure shapes public awareness of ransomware, or how ethical reasoning affects willingness to engage in or respond to cybercrime. Research should also examine the accessibility challenges older adults face with digital surveys and explore alternative data collection methods. Finally, researchers should incorporate theoretical underpinnings in their studies.

Acknowledgements

We used ChatGPT to correct grammatical errors in our paper.

References

Association, N. M. (2023). Ransomware as a service: What you need to know to protect against a growing threat.

Baker, K. (2023, January 30). Ransomware as a Service (RaaS) explained: How it works & examples. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Borghare, P. T., Methwani, D. A., & Pathade, A. G. (2024). A comprehensive review on harnessing wearable technology for enhanced depression treatment. Cureus.

Chen, J., Yuan, D., Dong, R., Cai, J., Ai, Z., & Zhou, S. (2024). Artificial intelligence significantly facilitates development in the mental health of college students: A bibliometric analysis. Frontiers in Psychology.

Chuchu, T., & Ndoro, T. (2019). An examination of the determinants of the adoption of mobile applications as learning tools for higher education students. International Journal of Interactive Mobile Technologies, 13(9), 53–67.

Dhingra, L. S., Aminorroaya, A., Oikonomou, E. K., Nargesi, A. A., Wilson, F. P., Krumholz, H. M., & Khera, R. (2023). Use of wearable devices in individuals with or at risk for cardiovascular disease in the US, 2019 to 2020. JAMA Network Open.

Fogel, J., & Nehmad, F. (2009). Internet social network communities: Risk-taking, trust, and privacy concerns. Computers in Human Behavior, 25(1), 153–160.

GlobalSign. (2023). A multi-layered approach to cybersecurity.

Halcyon. (2024). Power rankings: Ransomware malicious quartile (Q4 2024).

Huhn, S., Axt, M., Gunga, H.-C., Maggioni, M. A., Munga, S., Obor, D., … Barteit, S. (2022). The impact of wearable technologies in health research: Scoping review. JMIR mHealth and uHealth.

IBM. (2023). Physical cybersecurity: Protecting the intersection of digital and physical assets.

Moore, M. (2022, December 14). 45 Cybersecurity statistics and facts for 2025. University of San Diego. https://onlinedegrees.sandiego.edu/cyber-security-statistics/

Palatty, N. J. (2025, January 9). 100+ Ransomware attack statistics 2025: Trends & cost. Astra Security. https://www.getastra.com/blog/security-audit/ransomware-attack-statistics/

Pei, J., Amanvermez, Y., Vigo, D., Puyat, J., Kessler, R. C., Mortier, P., … Cuijpers, P. (2024). Sociodemographic correlates of mental health treatment seeking among college students: A systematic review and meta-analysis. Psychiatric Services, 75(5), 556–569.

Research, P. (2019). U.S. generations and technology use. Pew Research Center. https://www.pewresearch.org

Sano, A. (2016). Measuring college students' sleep, stress, mental health, and wellbeing with wearable sensors and mobile phones. (Doctoral dissertation, Massachusetts Institute of Technology).

Security, U. D. (2024). Feature article: Leveraging AI to enhance the nation's cybersecurity.

Tatu, C. (2024, December 20). Wearable tech: A game changer for athletes' performance. Lehigh University News. https://news.lehigh.edu/wearable-tech-a-game-changer-for-athletes-performance

Ubrani, J., Reith, R., & Llamas, R. T. (2025, April 28). IDC's worldwide wearable vendor market data. International Data Corporation. https://www.idc.com/promo/wearablevendor

Vonage. (2023). The generational gap in cybersecurity and privacy. https://www.vonage.com

Webroot. (2024). Battle of the generations: Ransomware. https://www.webroot.com

Xu, Y., Peng, J., Jing, F., & Ren, H. (2024). From wearables to performance: How acceptance of IoT devices influences physical education results in college students. Scientific Reports, 14, 1234–1246.

Yosep, I., Suryani, S., Mediani, H. S., Mardhiyah, A., & Ibrahim, K. (2024). Types of digital mindfulness: Improving mental health among college students – A scoping review. Journal of Multidisciplinary Healthcare, 17, 43–53.

Appendix A: Survey Questions

Demographic Information
DI1. What is your age?
DI2. What is your gender?
DI3. What is your highest level of education?
DI4. What is your current occupation?
DI5. On a scale of 1 (Not at all confident) to 5 (Extremely confident), how confident are you in your understanding of ransomware?
DI6. How many computer science or cybersecurity courses have you completed?

Perception of RaaS across generation (1 = Strongly disagree and 5 = Strongly agree)
ConcernedThreat: I am concerned about ransomware threats.
KnowRaas: I was familiar with Ransomware-as-a-Service (RaaS) before this survey.
DiffGenPercieve: I believe that different generations perceive ransomware threats differently.
MyGenVuln: My generation is more vulnerable to ransomware attacks than other generations.
Training: I participated in cybersecurity training or education.
ExpRansAttck: I know someone who has experienced a ransomware attack.
ClickLinks: I click on unfamiliar links or attachments.
YoungThanOld: I think younger generations are more likely to understand ransomware threats compared to older generations.
MyGenAware: People in my generation are generally aware of RaaS and its risks.

Attitudes Toward Paying Ransoms (1 = Strongly disagree and 5 = Strongly agree)
PayRans: I would pay a ransom to recover it if my personal data were encrypted in a ransomware attack.
PayEncAttack: Paying ransom encourages more cybercrimess.
CriticalInfa: If a hospital or emergency service provider were attacked by ransomware, I would support them paying a ransom to restore critical services
GovInter: The government should be involved in ransomware incident responses.
MyGenPays: People in my generation are more likely to pay a ransom than other generations.
MyGenValueMore: My generation places a higher value on digital data than older generations.
WillingToPayAmt: How much money would you be willing to pay to recover your personal files if attacked? (Multiple choice scale)
FactorInfluencePayment: If you lose your files or your files are encrypted what factors would influence your decision to pay a ransom? (multiple choice options: Value of data, Ransome amount, Likelihood of recovery, Legal considerations, Law enforcement advice, Time sensitivity, Trust in the attacker's promise to decrypt data)

Motivations for Engaging with RaaS (1 = Strongly disagree and 5 = Strongly agree)
ConsiderRaaS: I have considered engaging in cybercrime such as using RaaS.
YoungGenInvolv: Younger generations are more likely to get involved in RaaS activity.
RaaSAds: I have been approached or have seen advertisements for Ransomware-as-a-Service on the internet.
BuyRaaSEasy: I think it is easy for someone to purchase or use Ransomware-as-a-Service.
SocioEcon: Individuals may use RaaS because of financial hardship or economic pressure.
RaaSForFun: Individuals might use RaaS for fun or experimentation.
NoRisk: People are more likely to engage in RaaS if there is little chance of getting caught.
MyGenLessLikely: People in my generation are less likely to engage in RaaS than other generations.