# UNDERGRADUATE BUSINESS STUDENT ONLINE ATTITUDE AND BEHAVIOR: AN EMPIRICAL EXAMINATION OF THE COVID-19 PANDEMIC EFFECTS

**Carl J. Case, St. Bonaventure University**
**Darwin L. King, St. Bonaventure University**

## ABSTRACT

*Phishing has been an ongoing challenge for both individuals and organizations. Of particular concern to information systems educators are the attitudes and online behavior of the next corporate users, our current business students. This study was therefore conducted to empirically examine the aspects of spyware, phishing, and identity theft and, in particular, if there are COVID-19 pandemic effects. Results suggest that online minutes have greatly increased, concern about spyware has decreased, and concern about identity theft has increased since the beginning of the pandemic. However, no statistically significant correlation between online minutes and behavior was found.*

Keywords*: phishing, identity theft, undergraduate students, empirical study*

## INTRODUCTION

Spyware is one of the oldest and most widespread online threats in which the computer is secretly infected to initiate a variety of illegal activities including identity theft or a data breach (Malwarebytes.com, 2022). Techniques include phishing, spoofing, using Trojan horses, exploiting security vulnerabilities such as back doors, and so on.

In terms of identity theft, the Aite-Novarica Group found that 47% of Americans experienced financial identity theft in 2020. And, the Federal Trade Commission's (FTC) Consumer Sentinel Network analysis of over 5.7 million complaints in 2021 found that 25% were for identity theft (Insurance Information Institute, 2022). The most common types of identity theft were for government benefits applied for/received (31%) and credit card fraud for new accounts (29%).

Data threats can be manifested in several forms such as ransomware, targeted hacking, vendor or customer impersonation, IP address hacking, extortion, and so on (Neustar, 2018). The most recent noteworthy data breaches include: the 2021 LinkedIn data breach exposing the personal information of 700 million users (93% of all LinkedIn members), the March 2021 attack on Microsoft that affected more than 30,000 U.S. businesses and government agencies, the 2021 infiltration of the Colonial Pipeline Company with ransomware that caused fuel shortages across the U.S., and the ransomware attack of the meat processing company JBS that shut down beef and poultry processing plants on four different continents (Sobers, 2022).

The IBM Security (2021) Data Breach Report estimates the average cost of a data breach is $4.24 million. Data breaches that take longer than 200 days to identify and contain cost on average $4.87 million as compared to $3.61 million for breaches that take less than 200 days. Overall, the report found it takes an average of 287 days to identify and contain a data breach. Ransomware attacks, for example, cost an average of $4.62 million which includes escalation, notification, lost business, and response costs, not including the cost of the ransom.

According to Verizon's Data Breach Investigative Report 2022 analysis of over 23,000 cybersecurity incidents and 5,200 confirmed breaches from around the world, 25% of all data breaches involve phishing and 85% of data breaches involve a human element (Verizon.com 2022). Moreover, the FBI's Internet Crime Complaint Center (IC3) found that phishing, including vishing, SMiShing and pharming, was the most prevalent threat in the U.S. in 2020, with 241,342 victims (Jones, 2022). This was followed by non-payment/non-delivery (108,869 victims), extortion (76,741 victims), personal data breach (45,330 victims) and identity theft (43,330 victims). This is problematic given that Terranova Security's 2020 Gone Phishing Tournament found nearly 20% of all employees are likely to click on phishing email links and, of those, 67.5% go on to enter their credentials on a phishing website.

Phishing mechanisms continue to evolve. A new form is through the use of Quick Response (QR) codes (Bergal, 2022). In January of 2022, the FBI issued an alert about cybercriminals tampering with posted QR codes to steal login and financial information. Pay-to-park kiosks, for example, have been targeted with criminals slapping stickers with fake QR codes on pay stations. Fake codes are then used to redirect payments and embed malware in the unsuspecting victim's mobile device.

According to Check Point, in the fourth quarter of 2020, Microsoft was the most impersonated brand globally when it comes to brand phishing attempts, accounting for 43% of the attempts (checkpoint.com, 2020). Attackers are likely exploiting Microsoft's name given the increase in organizations relying on Microsoft's suite of cloud applications since the start of the pandemic. Other brands impersonated include DHL (18% of attempts), LinkedIn (6% of attempts), and Amazon (5% of attempts). Unfortunately, email security provider Ironscales' State of Cybersecurity Survey poll of more than 400 U.S. IT professionals found that 81% of respondents experienced an increase in email phishing attacks since the start of the pandemic, from March 2020 to September 2021 (Thomas, 2021). And, only 19% of organizations provide cybersecurity awareness training on an annual basis.

Given the increasing incidences of phishing, data breaches, and identity theft, the study was conducted to examine the attitude, incidence, and trends relative to undergraduate business students. This empirical study examines several questions. Are students concerned about spyware and identity theft? What are student online activity minutes? Are students protected with a second firewall? Have students responded to phishing email and/or have been a victim of identity theft? And, has the March 11, 2020 World Health Organization declaration of the novel coronavirus (COVID-19) as a global pandemic changed attitudes and activity (Cucinotta & Vanelli, 2020)? Results are important in better understanding the state of student online behavior and if modifications to student education are needed to minimize vulnerability.

## PREVIOUS RESEARCH

An initial study by the authors conducted in 2006-2007 found that only 26% of undergraduate students indicated receiving phishing email with 16 phishes received per month per student (Case and King, 2008). A subsequent study conducted 2007-2010 examined email quantity (King & Case, 2012). Results demonstrated that students received 212 emails per month with the largest category, 35%, being unsolicited or spam emails. Class-related (26%), personal/non-class (13%), and other email (26%) were less common. A third study by the authors conducted 2011-2015 examined types of phishing (Case & King, 2016). Responses illustrate that for every year of the study, credit card phishing emails were the most common type of attack with 18-23% of students per year indicating receiving them. Amazon.com (14-19%), eBay (8-12%), Nigerian Scam (6-10%), and other (4-5%) phishes were also received.

To predict user susceptibility to phishing websites, Abbasi, et.al (2021) proposed and tested the phishing funnel model (PFM). PFM incorporates user, threat, and tool-related factors to predict actions during four key stages of the phishing process: visit, browse, consider legitimate, and intention to transact. Experiments demonstrated PFM significantly outperformed competing models/methods by correctly predicting visits to high-severity threats 96% of the time. In addition, a follow-up field study revealed that employees using PFM were significantly less likely to interact with phishing threats relative to comparison models and baseline warnings.

Furthermore, because scammers may use a step by step approach to gain a potential victim's trust, Abroshan, et.al (2021) investigated the extent risk-taking and decision-making styles influence the likelihood of phishing victimization in such instances. Results suggest that the attitude to risk-taking and gender can predict users' phishability in the different steps selected.

In terms of spyware, Sideri et al. (2019) used a case study to investigate the privacy literacy of university students in relation to the usage of social media. Researchers held a thirteen-week course on social media with the goal of strengthening privacy literacy. Although the students at the outset did not have the necessary knowledge in this field, after completing the course participants exercised more caution with regard to their profile visibility, paid more attention to the privacy settings of Facebook, and had increased awareness of the usefulness of anti-spyware software.

Relative to identity theft, Ogbanufe & Pavur (2022) explored why and how individuals adaptively and maladaptively respond to the threat. The researches provided empirical evidence of conditions under which fear and regret motivate personal security protection measures, thus enabling practitioners to promote identity theft protection more efficiently. Results suggest that fear is only effective when the threat is high and anticipated regret is effective in both high and low threat conditions. Also, anticipated regret has the most potent effect on increasing adaptive coping responses in a low threat model. Thus, anticipated regret rather than fear could be used in situations where the threat is low.

Finally, Salam, et.al (2021) proposed an empirical assessment of the construct of user control over identity theft. Findings suggest that when users have the perception of more control over the identity theft threat, they are likely to find solutions, feel it is their responsibility, and have more intentions for identity theft prevention actions to prevent identity theft.

## RESEARCH DESIGN

This study employs a survey research design. The research was conducted at a private, northeastern U.S. university. A Student Phishing instrument was developed by the authors and administered each semester during a five-year period (from spring 2018 through spring 2022) to undergraduate students enrolled in a School of Business course. However, because of the university unanticipated face-to-face instruction discontinuance midway through the spring of 2020, no data were collected during that semester. The courses included a variety of subjects such as Business Information Systems, Introduction to Financial Accounting, Introduction to Managerial Accounting, Macroeconomics, and Business Policy. A convenience sample of class sections and faculty members was selected to minimize the probability of a student receiving the survey in more than one class and to ensure consistency, the same questions were asked during each of the semesters. Because of the sensitivity of the subject and to encourage honesty, no personally-identifiable data were collected and respondents were informed that surveys were anonymous, participation was voluntary, and responses would have no effect on his/her course grade. In addition, students were asked to complete the survey only one time per semester. Prior to the pandemic, the surveys were completed via paper in an academic classroom. Subsequent to the beginning of the pandemic, the surveys were completed via an online link.

The survey instrument was utilized to collect student demographic data such as gender and academic class. In addition, the survey examined student Internet behavior regarding shopping, non-school related surfing, phishing, spyware, firewalls, and identity theft. Results were summarized by activity and correlations were calculated to determine potential relationships between online minutes and behaviors. To examine potential trends, the data was segmented by calendar year. However, because of the anonymity of respondents, it could not be determined if a given student participated during multiple semesters so repeated measures were not examined.

## RESULTS

A sample of 952 usable surveys was obtained. As indicated in Table 1, 60% of the respondents were male and 40 were female. These percentages were fairly consistent with the study university's School of Business student population.

**Table 1**
**Gender Response Rate by Year**

| | 2018 | 2019 | 2020 | 2021 | 2022 | Total |
|---|---|---|---|---|---|---|
| Male | 59% | 60% | 67% | 58% | 65% | 60% |
| Female | 41% | 40% | 33% | 42% | 35% | 40% |
| Count | 311 | 344 | 80 | 155 | 62 | 952 |

The response rate by academic class was relatively equally distributed. As indicated in Table 2, 18% of respondents were freshmen, 36% were sophomores, 30% were juniors, and 16% were seniors.

**Table 2**
**Academic Class Response Rate by Year**

| | 2018 | 2019 | 2020 | 2021 | 2022 | Total |
|---|---|---|---|---|---|---|
| Freshmen | 21% | 28% | 0% | 4% | 10% | 18% |
| Sophomore | 36% | 32% | 23% | 41% | 55% | 36% |
| Junior | 28% | 17% | 70% | 46% | 26% | 30% |
| Senior | 15% | 8% | 8% | 9% | 10% | 16% |

Responses were first examined with regard to the student's level of concern about spyware. As indicated in Table 3, in 2018, 16% strongly disagreed, 22% disagreed, 28% were neutral, 20% agreed, and 10% strongly agreed with respect to being concerned about spyware. At the onset of the pandemic in 2020, 24% strongly disagreed, 33% disagreed, 19% were neutral, 23% agreed, and 6% strongly agreed about his/her concern. By 2022, 19% strongly disagreed, 31% disagreed, 21% were neutral, 21% agreed, and 8% strongly agreed about his/her concern. Results demonstrate that the percent of students concerned about spyware was relatively consistent from 2018 to 2022 with 30%, 28%, 29%, 30%, and 29%, respectively, of students indicating concern. On the other hand, the percentage not concerned varied from 2018 to 2022 to 38%, 37%, 57%, 39%, and 50%, respectively, of students.

**Table 3**
**Concerned About Spyware by Year**

| Level of Agreement | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| Strongly Disagree | 16% | 13% | 24% | 14% | 19% |
| Disagree | 22% | 24% | 33% | 25% | 31% |
| Neutral | 28% | 30% | 19% | 32% | 21% |
| Agree | 20% | 19% | 23% | 21% | 21% |
| Strongly Agree | 10% | 9% | 6% | 9% | 8% |

Next, responses were examined with regard to the student's level of concern about identity theft. As indicated in Table 4, in 2018, 8% strongly disagreed, 31% disagreed, 47% were neutral, 13% agreed, and 3% strongly agreed with respect to being concerned about identity theft. At the onset of the pandemic in 2020, 18% strongly disagreed, 34% disagreed, 20% were neutral, 28% agreed, and 5% strongly agreed about his/her concern. In terms of identity theft, from 2018 to 2022, 16%, 15%, 33%, 34%, and 26%, respectively, of students indicated concern. The percentage not concerned varied from 2018 to 2022 to 39%, 27%, 52%, 39%, and 46%, respectively, of students.

**Table 4**
**Concerned About Identity Theft by Year**

| Level of Agreement | **2018** | **2019** | **2020** | **2021** | **2022** |
|---|---|---|---|---|---|
| Strongly Disagree | 8% | 3% | 18% | 16% | 15% |
| Disagree | 31% | 24% | 34% | 23% | 31% |
| Neutral | 47% | 58% | 20% | 30% | 29% |
| Agree | 13% | 15% | 28% | 21% | 21% |
| Strongly Agree | 3% | 0% | 5% | 13% | 5% |

Activity minutes per day are presented in Table 5. Results illustrate that in 2018, respondents indicated spending 1 minute per day shopping online while spending 112 minutes per day engaged in non-school surfing. At the onset of the pandemic in 2020, respondents spent 3 minutes shopping and 221 minutes engaged in non-school surfing per day. By 2022, respondents spent 1 minutes shopping and 177 minutes engaged in non-school surfing per day. While shopping online minutes per day remained consistent at one minute per day from 2018 to 2022, non-school surfing varied from 112 minutes, 110 minutes, 221 minutes, 157 minutes, and 177 minutes per day, respectively, during the study years. Overall, total minutes per student increased from 107 minutes (1.8 hours) in 2018 to 165 minutes (2.8 hours) in 2022.

**Table 5**
**Activity Minutes Per Day by Year**

| **Activity** | **2018** | **2019** | **2020** | **2021** | **2022** |
|---|---|---|---|---|---|
| Shopping Online | 1 | 1 | 3 | 1 | 1 |
| Non-School Surfing | 112 | 110 | 221 | 157 | 177 |
| Total | 107 | 105 | 219 | 154 | 165 |

Respondent behavior was further examined and presented in Table 6. In 2018, 6% indicated responding to a phishing email in the past year, 27% indicated using a second firewall, 4% indicated being a victim of identity theft, and 26% indicated personally knowing a victim of identity theft. At the onset of the pandemic in 2020, 7% indicated responding to a phishing email in the past year, 17% indicated using a second firewall, 7% indicated being a victim of identity theft, and 37% indicated personally knowing a victim of identity theft. By 2022, 2% indicated responding to a phishing email in the past year, 11% indicated using a second firewall, 5%

indicated being a victim of identity theft, and 53% indicated personally knowing a victim of identity theft. With respect to behavior, in general, the majority of students did not exhibit any of the behaviors during each of the five years. For example, from 2018 to 2022, only 6%, 6%, 7%, 8%, and 2%, respectively per year, of students responded to a phishing email during the past year. Moreover, only 4%, 11%, 7%, 7%, and 5%, respectively per year, of students have been a victim of identity theft. Second firewall usage was more common each year, respectively, with 27%, 35%, 17%, 14%, and 11%, respectively per year, of students indicating this behavior. Personal knowledge of an ID theft victim was also more common with 26%, 24%, 37%, 38%, and 53%, respectively per year, of students indicating this knowledge.

**Table 6**
**Behaviors by Year**

| **Behavior** | **2018** | **2019** | **2020** | **2021** | **2022** |
|---|---|---|---|---|---|
| Responded to Phishing Email in Past Year | 6% | 6% | 7% | 8% | 2% |
| Use a Second Firewall | 27% | 35% | 17% | 14% | 11% |
| Have Been Victim of Identity Theft | 4% | 11% | 7% | 7% | 5% |
| Personally Know an ID Theft Victim | 26% | 24% | 37% | 38% | 53% |

Finally, potential correlations between the quantity of surfing minutes and various behaviors were examined in Table 7. Statistically significant Spearman Rho correlations were not found with respect to any behavior including responding to a phishing email in the past year, using a second firewall, or being a victim of identity theft.

**Table 7**
**Spearman Rho Correlations between Surfing Minutes and Behavior**

| Behavior | Correlation Coefficient |
|---|---|
| Responded to Phishing Email in Past Year | -.188 |
| Use a Second Firewall | .132 |
| Have Been Victim of Identity Theft | .082 |

* Correlation is significant at .05 level (2-tailed).
** Correlation is significant at .01 level (2-tailed).

The limitations of these results are primarily a function of the sample, sample distribution, and type of research. The use of additional universities, a more equal distribution among gender, and increased freshman participation would increase the robustness of results. Another limitation relates to the self-reported nature of the survey.

## IMPLICATIONS

There are three important implications from the study. One implication relates to student attitude. Prior to the pandemic, a minority, 36-37%, of students per year were not concerned about spyware. However, at the onset of the pandemic, the majority, 57%, of students indicated a lack of concern. This lack of concern remained at 50% of students by the end of the pandemic. It is possible the social isolation and life traumas associated with the pandemic resulted in an increased sense that online privacy is not as important as the other life and death challenges associated with a pandemic. Another aspect of the pandemic relates to concerns about identity theft. Prior to the pandemic, 15-16% of students indicated concern. However, at the onset of the pandemic, this percentage more than doubled to 33%. At the end of the pandemic, the percentage decreased to 26%, but remains much larger than the pre-pandemic years. It is possible that the increased dependence on and use of the Internet because of face-to-face COVID-19 exposure concerns and/or travel lock-downs during the pandemic has triggered the identity theft concern. These changes suggest that the pandemic has affected attitude related to both personal privacy and security threats.

A second implication is evident when examining behavior. While two behaviors, responding to a phishing email and being a victim of identity theft, have remained relatively small and consistent in occurrence during each of the five years, other behaviors have changed since the onset of the pandemic. Non-school surfing increased by 100% to 221 minutes per day during the first year of the pandemic and remained 54% higher at the end of the pandemic as compared to four years earlier. It likely that surfing increased because of the social isolation and/or increased discretionary time as a result of unemployment and tele-commuting. Another behavior, using a second firewall for intrusion detection/prevention, decreased by 50% to 17% at the onset of the pandemic and continued to decrease through the study years. This may also be a result of the feeling of social isolation and perception that one is not being spied upon.

Finally, the third implication relates to the difference in the level of identity theft victimization between students and others. While respondents indicated a dramatic increase in the knowledge of others being victimized (24% prior to pandemic, 37% at the onset, and 53% at the end of the pandemic), student victimization has varied slightly, from 4% to 11% per year, during the study. It is possible that either students are more aware of other’s victimization or are more vigilant because of education. This suggests that continued proactive education has been and may continue to be helpful in combating the scourge of identity theft. Future research will need to determine if the pandemic effects have permanently changed undergraduate student attitudes and behavior.

## REFERENCES

Abbasi, A., Dobolyi, D., Vance, A. & Zahedic, F. M. (2021). The phishing funnel model: a design artifact to predict user susceptibility to phishing websites. *Information Systems Research,* 32(2), June, 410–436, https://pubsonline.informs.org/doi/epdf/10.1287/isre.2020.0973

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9, 44928 – 44949, https://ieeexplore.ieee.org/abstract/document/9380285

Bergal, J. (2022). Think twice before scanning that QR code. *gnc.com*. February 22, https://www.gcn.com/cybersecurity/2022/02/think-twice-scanning-qr-code/362058/

Case, C. J. & King, D. L. (2016). Phishing: Are undergraduates at risk and prepared? *Issues in Information Systems*, 17(1), 80-88.

Case, C. J. & King, D. L. (2008). Phishing for undergraduate students. *Research in Higher Education Journal*, 1, 100-106

Checkpoint.com (2020. Brand phishing report – Q4 2020. *Checkpoint.com*, https://blog.checkpoint.com/2021/01/14/brand-phishing-report-q4-2020/

Cucinotta, D. & Vanelli, M. (2020). WHO declares COVID-19 a pandemic. *Acta Biomed*, 91(1), 157-160, https://pubmed.ncbi.nlm.nih.gov/32191675/

IBM Security (2021). Cost of a data breach report 2021. *Expertinsights.com*, https://expertinsights.com/insights/50-phishing-stats-you-should-know/

Insurance Information Institute (2022). Facts + statistics: Identity theft and cybercrime. *Iii.org*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

Jones, C. (2022). 50 phishing stats you should know in 2022. *Expertinsights.com*, April 20, https://expertinsights.com/insights/50-phishing-stats-you-should-know/

King, D. L. & Case, C. J. (2012). The student's decision of whether or not to go phishing. *Business Research Yearbook, Global Business Perspectives*, XIX(1), 72-79.

Malwarebytes.com (2022). All about spyware. *Malwarebytes.com*, https://www.malwarebytes.com/spyware

Ogbanufe, O. & Pavur, R. (2022). Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management*, 62, February, 1-17, https://www.sciencedirect.com/science/article/pii/S0268401221001250#!

Salam, A.F., Dai, H. & Wang, L. (2021). Online users' identity theft and coping strategies, attribution and sense of urgency: a non-linear quadratic effect assessment. *Information Systems Frontiers*, https://doi.org/10.1007/s10796-021-10194-w

Sideri, M, Kitsiou, A., Tzortzaki, E., Kalloniatis, C., & Gritzalis, S. (2019). Enhancing university students' privacy literacy through an educational intervention: A greek case-study. *International Journal of Electronic Governance*, 11(3–4), 333–360, https://doi.org/10.1504/IJEG.2019.10018628

Sobers, R. (2022). 166 Cybersecurity statistics and trends [updated 2022]. *Varonis.com,* July 8, https://www.varonis.com/blog/cybersecurity-statistics

Thomas, I. (2021). IRONSCALES releases findings from the state of cybersecurity survey, October 15, https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/

Verizon.com (2022). 2022 data breach investigations report. *Verizon.com*, https://www.verizon.com/business/en-gb/resources/reports/dbir/