Article Summaries

Follow this and additional works at: https://scholarsarchive.byu.edu/joni

Part of the Civic and Community Engagement Commons, International Relations Commons, and the Nonprofit Administration and Management Commons

Recommended Citation
Available at: https://scholarsarchive.byu.edu/joni/vol3/iss3/2

This Literature Reviews is brought to you for free and open access by the Journals at BYU ScholarsArchive. It has been accepted for inclusion in Journal of Nonprofit Innovation by an authorized editor of BYU ScholarsArchive. For more information, please contact ellen_amatangelo@byu.edu.
The Journal of Nonprofit Innovation

An Online Journal for Reviews of Academic Research and Thought Papers on Community and Global Issues

Edition: Online Protection of Children
- Latest Research (Summaries)
- Article: An NPO's Values and Identity
- Nonprofit & Partnership Spotlights

Published by BYU ScholarsArchive, 2023
Acknowledgments

Editorial Board Lead
Angie Holzer, EdD
CEO/Founder, WikiCharities

Professional Review Board
Angie Holzer, EdD
Beverli J. DeWalt
Hannah Cheng, MS
Heather Hammond Cruz, MBA
Jane Mitchell, JD
Patrick Panos, PhD
Rachel George, PhD
Ria Roy, PhD

Chief Editor
Marianna Richardson, PhD

Associate Editor
Seth Martinez, PhD

Student Chief Editor
Erica Bassett

Student Editorial Team
Erica Bassett
Haoming Song
Mandie Carter
Aditya Manoj Menon

The Journal for Nonprofit Innovation is a publication of WikiCharities, a 501c3 nonprofit.

© 2023 WikiCharities. All rights reserved.

info@wikicharities.org
wikicharities.org
Bountiful, Utah USA

All images pulled from Unsplash and Pexels.
# TABLE OF CONTENTS

## ABOUT JONI ................................................................. 4

## LATEST RESEARCH (ARTICLE SUMMARIES) ................................................................. 5

**Summary 1**: The Emergence of Deepfake Software-Compromising Cybersecurity .......... 6
**Summary 2**: Just Techno-Panic or a Real Risk? Publishing Children’s Pictures Online: A Review of Literature ......................................................... 8
**Summary 3**: How Can Cybercrime Atlas Fight Off Cybercrime? ............................... 10
**Summary 4**: Sharenting Syndrome: An Appropriate Use of Social Media? ........ 12
**Summary 5**: Children’s Online Safety: Predictive Factors of Cyberbullying and Online Grooming Involvement ......................................................... 14
**Summary 6**: A Critical Analysis of Fraud Cases on the Internet ............................. 15
**Summary 7**: How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails ......................................................... 17
**Summary 8**: Teachers’ Management of Cyberbullying on China’s Social Media Sites: A Case Study in Shandong Province, China ......................................................... 18

## RESEARCH AND THOUGHT PAPERS ................................................................. 21

**Online Safety Laws by Country** ................................................................................. 22
**The Power of Protective Factors: A Framework for Mental Health Action and Education** .................................................................................................. 29
**An NPO’s Values and Identity** ..................................................................................... 35
**Investigating the Potential Benefits of Standards-Based Grading Practices at Urban Secondary Schools in Southern Utah: A Qualitative Study** 45
**Factors Influencing Employer Satisfaction in Nonprofit Organizations in the United States** .................................................................................................. 50
**Feminist Pragmatism in the Nonprofit Sector** ........................................................... 56

## NONPROFIT & PARTNERSHIP SPOTLIGHTS ................................................................. 60

**KMS Foundation** .................................................................................................. 61
**Venturefy** ................................................................................................................. 62
**Maxsip: Free Internet (United States)** ........................................................................ 64

## ISSUE TOPICS AND SUBMISSION DETAILS ................................................................. 65

---

*JoNI: Journal of Nonprofit Innovation* 

September 2023, Vol 3, Iss 3 

Published by BYU ScholarsArchive, 2023
**About JoNI**

The Journal of Nonprofit Innovation (JoNI) is a publication of WikiCharities, a US-based 501c3 nonprofit organization dedicated to nonprofit transparency and collaboration in partnership with Brigham Young University (BYU). JoNI is an online journal for academic research summaries and thought papers on community and global issues. We exist to help nonprofit leaders know the latest research and collaborate on their experiences.

**Our Mission**

The Journal of Nonprofit Innovation (JoNI) provides a way for nonprofit leaders to stay up to date on the latest research and collaborate, building a more innovative and collaborative nonprofit sector.

**Submissions**

For more information on how to get involved or how to submit pieces for upcoming issues, visit us online at journalofnonprofitinnovation.org.
Latest Research (Summaries)

Focus: Online Protection & Safety
Summary 1
The Emergence of Deepfake Software-Compromising Cybersecurity


Abstract
One of the fastest growing fields in recent technology is artificial intelligence (AI). While AI has helped automate many repetitive tasks or simple tasks (which has led to increase in overall productivity in various fields), AI systems are usually tuned to personalize user experience, thus improving customer satisfaction. Moreover, AI systems/algorithms can analyze and draw accurate deductions and trends, which might be impossible for humans to identify, and which is crucial for making informed business decisions.

However, with the emergence of any type of technology comes their drawbacks and threats to cybersecurity. One such example is the emergence of Deepfakes, which uses a combination of machine learning and artificial intelligence technologies to mimic/manipulate the audio and visuals of a person (usually unauthorized during cyberattack). This software poses risk to individuals, because it can be manipulated to spread fake information/propaganda, which would stain their public image.

Background
Cybercriminals have taken full advantage of Deepfake technology over recent years due to the major developments and realism of the product. Improved graphics paired up with artificial intelligence personalized functions help the Deepfake user manipulate the voices and actions videos or images. Deepfakes were initially used in the movie industry to make edits on the actors and give the movie that finishing touch. However, this technology has been misused over the past few years. For instance, a study conducted in Amsterdam-based company Deeptrace Labs shows that 96% of Deepfake videos were pornographic in nature, and most of them were Deepfakes of women. This has been used as a blackmailling technique by cybercriminals, especially targeting young children and adults.

The core of Deepfake technology is created using two principles of machine learning, which are artificial neural networks called the “generator” and the “discriminator.” The artificial neural network is used to replicate human brain functions, such as being able to understand and make facial expressions. The data of various images and videos are used to help improve the Deepfake system’s ability to understand and create fake samples. The better the resolution and quality of the videos and images, the better the performance of the system. The generator creates a fake video using imaging and video editing, and then the discriminator tries to distinguish between the real and fake video. When it does, the generator will make incremental improvements and the discriminator will try to distinguish between the two again, and the cycle continues until the discriminator can no longer differentiate between the fake and real video, which would imply that the fake video would be seamless and indistinguishable by the naked eye. The same is applicable for Deepfake-generated photos.

Various agencies and individuals around the globe that have their personal vendetta try to spread misinformation to cause havoc between institutions and citizens. Many foreign countries have conducted disinformation campaigns to deceive citizens and weaken foreign affairs. For example, the Russian IRA had employed individuals and organizations to acquire the social media accounts of various US citizens. This was an attempt by the Russians to spread fake news to deceive the citizens and turn them against the US.
The use of Deepfake made fake news more believable and dangerous. Moreover, politicians are afraid that Deepfake would be used to manipulate what they say and spread fake news across various social media platforms. A very famous Deepfake video was made by comedian Jordan Peele, who used Deepfake to portray the former president Barack Obama delivering a public announcement. The video was intended to be entertaining but was also intended to bring awareness to the issue of the potential risks and the realism of this technology.

A study conducted by Pew Research showed that over 55% of adults get their news from various social media platforms, therefore circulation of fake news on different social media platforms can alter the perspective of many adults. Moreover, it has been increasingly difficult to differentiate between authentic news and fake news. In addition to affecting the political system, Deepfakes also have affected various businesses and journal outlets, which struggle to figure out what types of data/information is genuine or fake.

Method
The author analyzed various articles related to Deepfake technology. Using relevant research and statistics, he showed the negative impacts of Deepfake technology. Moreover, he showed how deepfakes have been used in movie production, but also how it has been used by cybercriminals to taint other people’s images to spread fake news and potentially ignite hybrid warfare.

Takeaways
Deepfake technology has become more sophisticated over the years, allowing the unauthorized creation of auditory and visual content which can be used to spread misinformation in social media by cybercriminals. The scale of the threat of Deepfake technology is both at an individual and an intuitive and sometimes global level (in case of potential warfare) by eroding national security making it a serious concern for governments.

Moreover, Deepfake can be used to push an agenda since individuals are more inclined to believe what is presented on social media. Therefore, cybercriminals can take advantage of that and spread misinformation that a biased person would perceive as real information. Moreover, Deepfake can be used to manipulate a politician’s words which would have a significant impact on shaping public opinion. However, the most common use of Deepfakes is on pornographic content, where usually female public figures’ faces are edited into existing video, thereby tampering their social image.

Summary
Just Techno-Panic or a Real Risk?
Publishing Children’s Pictures Online: A Review of Literature


Abstract
“The Internet has become an essential resource for social interaction among children, but it brings with it both advantages and disadvantages that depend in part on how it is used. This study, which is anchored in social learning theory, employed a desktop review of existing literature that focused on Kenya but covered global and other regional levels as well. The study found several benefits of the Internet for children: updating family and friends on new developments in the children’s lives, reviewing photos and other records of past events, engaging in online interactions, and increasing their capacity for learning. Nonetheless, there are also Internet-specific risks, such as access to inappropriate content and unsafe interactions with other children or adults. Other risks include “digital kidnapping” and contact with perpetrators who encourage children to engage in sexual activity. Although some countries have policies on Internet usage, few have specific policies or guidelines addressing children’s vulnerability when sharing their pictures online. Moreover, most such policies are not applied in practice, especially in African countries. The study recommends developing and implementing policy frameworks to protect children online and using privacy settings to protect their information.”

Background
“Sharenting” is the practice where parents constantly post pictures of their children on social media for the entirety of the internet to see. It has become incredibly prevalent over the past few years. A survey conducted in the United States indicates that 56% of mothers and 34% of fathers have shared pictures of their children on social media. The survey also states that “The majority of parents who use social media (74%) know of another parent who has shared too much information about a child on social media, including parents who gave embarrassing information about a child (56%), offered personal information that could identify a child’s location (51%), or shared inappropriate photos of a child (27%)” (2), demonstrating how prevalent it has become for parents to be sharing information about their children on the internet, and at times incredibly excessive amounts.

With social media usage becoming increasingly common in the world, concerns naturally arose about the privacy of sharing information on social media, especially for young children. Various countries around the world have come up with different laws and policies to protect data and children on the internet. The Children’s Online Privacy Protection Act (COPPA), passed in 1998 by the United States, was designed to protect the online privacy of children under 13, by websites
requiring parental consent before obtaining data on their children. The European Union established the Safer Internet Plus Programme that seeks to create a safe internet environment for children through the filtering of content that could potentially be mentally harmful for their eyes. The United Nations Convention on the Rights of the Child states that children have the right to (Santos Pais & Bissell, 2006).

There are many such laws protecting child online privacy in Africa as well. Laws like the Rwanda Child Online protection policy and Data Protection Act in Kenya were designed to prevent the misuse of data regarding children’s information online. Section 8 of the Child Rights Act in Nigeria’s constitution states children’s rights to privacy, and Section 23 of the Cybercrimes Act in 2015 punishes child pornography and criminalizes cyberbullying. However, research has shown that these laws have not been implemented effectively.

Recently, people have become worried that parents’ habits of sharing photos of their children online without their consent does not create a good outlook on them being role models for their children, along with other concerns related to sharing personal information online. These studies seek to wonder if this concern has valid reasoning or is just a “technopanic,” a widespread fear elicited from the mass spreading of technology that does not have scientific proof to back it up.

**Methods**
The author performed a desktop literature review and searched for studies that had relevant content on sharenting and the protection of children’s online privacy. Using Google Scholar and Scopus as search material, they chose and read 52 articles concerning the matter, with a focus on studies in Kenya. The relevant themes included the advantages and disadvantages of sharing children’s photos online and policies put in protection of children on the internet.

**Takeaways**
A study found that 44% of children in Spain have experienced at least one instance of sexual harassment online, and another found that 20% of children have experienced some form of cyberbullying (77-78). Additionally, another study found that “nearly a third of the public secondary students who participated in their survey felt that sexting on mobile phones was the social media usage that had the most influence on the rate of teenage sex” (80). It can be clearly seen that verbal and sexual harassment and exploitation are among the greatest risks of sharing children’s information and photos on the internet. It’s important that parents adapt steps to address these situations through techniques like: “(a) the use of privacy settings to protect children’s information, (b) alternative ways of sharing pictures, (c) protocols on the use and sharing of children’s photos in schools, (d) avoiding the use children’s names along with images, and (e) turning off location settings on devices used to share pictures online” (81-82).

At the same time however, sharenting provides a great medium for parents to connect with each other over life stories and even help each other with difficult situations and giving each other advice. For example, sharing photos and information helps families who are physically separated from each other to remain socially connected. A study conducted in Pakistan even found internet use to be beneficial for children,
helping them boost confidence, self-esteem, and social skills (79).

Finally, the study found that while there were abundant sources of information on the benefits and risks of sharenting and child internet use in European countries and the United States, there was scarce information available in African countries like Kenya, which creates a knowledge gap between the regions and suggests that data protection laws have not been properly implemented in Africa. More effort needs to be done by policymakers in order to correct the gap and ensure the safety of children in these countries.


Summary 3
How Can Cybercrime Atlas Fight Off Cybercrime?


Abstract
“Over the past two decades, the number of cybercrimes has skyrocketed with increased digitization of almost every aspect of our lives. This digitization includes not only personal communication and financial transactions but also critical infrastructure, healthcare systems, transportation, and even national defense—all of which have become reliant on interconnected digital technologies. Moreover, increased improvement or rapid growth of technology has provided more opportunities for cyber criminals to emerge and take advantage of the loopholes in these new technologies for monetary gains or stealing data. In addition, increased connectivity has enabled cybercriminals to easily connect/communicate with their potential victims while disguising themselves as an ordinary person or a business partner. Therefore, in June 2022, the World Economic Forum (WEF) introduced the Cybercrime Atlas, an effort aimed at charting the actions of cybercriminals and establishing a global database that can assist law enforcement agencies in disrupting the cybercriminal network.”

Background
The Cybercrime Atlas was officially launched in February 2023, as a partnership between the WEF and some large companies such as Fortinet, Microsoft, and PayPal. The development of the Cybercrime Atlas began with the collaboration of skilled analysts from various organizations worldwide. They worked together to establish a standardized classification system and then selected samples for analysis, focused on 13 major known cybercriminal individuals or organizations. Analysts utilized open-resource intelligence to gather data such as the cybercriminals’ identities, known addresses, bank account and cryptocurrency wallet details, social media presence, and their use of malicious services like bulletproof hosting.

The primary goal was to compile all available open-source information on these individuals, normalize it, verify its authenticity, and create a centralized repository. Glenn Maiden, the director of threat intelligence operations at FortiGuard Labs ANZ, emphasized the importance of collecting and investigating this data to identify the most reliable information, filter out irrelevant details, and ensure the accuracy of the gathered intelligence.
The objective of the Cybercrime Atlas initiative is to construct a comprehensive overview of the cybercrime landscape, including criminal activities, shared infrastructure, and networks. The aim is to establish connections between the gathered information about cybercriminals, ultimately aiding the security industry and effectively disrupting the cybercriminal ecosystem.

Analysts were able to extract common data between the initial 13 criminal groups, including key attack areas such as ransomware, business email compromise, malware, and card fraud. The findings of this project will be shared with global law enforcement such as Interpol and the FBI. The insights derived from this effort are also expected to encourage greater collaboration between the private sector and law enforcement agencies to combat cybercrime. Moreover, the research has brought to light the collaboration of nation state entities and cybercriminals when carrying out and operating cybercriminal activities.

In February 2023, the Cybercrime Atlas was undergoing a transformation phase from a prototype to a viable product. There were dedicated project managers for this operation to find the most viable system to set up the database in and work out the business aspects to their decisions.

However, after development one of the main drawbacks is that non-Cybercrime Atlas partnering companies won’t be able to access the repository since the primary purpose of this project is to aid law enforcement to tackle cybercriminal attacks and not to commercialize the finding. Additionally, Fortinet, one of the project’s supporters, is exploring other opportunities and ways to disrupt cybercriminal activities, including potential legal or policy changes in jurisdictions where cybercriminals operate.

Methods
The author rigorously analyzed the creation and implementation of the Cybercrime Atlas. The author used a lot of factual explanation to convey the creation and purpose of the Cybercrime Atlas. Through thorough investigation of the Cybercrime Atlas, the author provides its future possible uses and how it would aid the law enforcement to help disrupt cyberattacks on individuals, public sectors, and private entities.

Takeaways
The Cybercrime Atlas is a database pioneered by the World Economic Forum (WEF) aimed at mapping the activities of cybercriminals. The development of the Cybercrime Atlas involved gathering information from open sources about known threat actors. Analysts focused on details like names, addresses, bank accounts, crypto wallets, and social media presence. The goal was to create a repository of normalized and verified information to build a comprehensive view of the cybercrime landscape. Initial efforts focused on collecting actionable intelligence from 13 criminal groups involved in various cyberattack types, including ransomware, business email compromise, malware, and card fraud. The collected information will eventually be shared with global law enforcement groups like Interpol and the FBI.

While primarily designed for law enforcement, the Cybercrime Atlas is still in development. It may provide opportunities for local law enforcement to enhance their intelligence. However, challenges such as dealing with threat actors providing false information remain to be
addressed. Though Cybercrime Atlas is a step in the right direction to lead with cyber-attacks, there are many challenges it needs to overcome to make it favorable to all parties.


Summary 4
Sharenting Syndrome: An Appropriate Use of Social Media?


Abstract
“The use of social media is on the rise, and posts about anything can be shared these days, whether it be clothes, jewelry, shoes, books, or food and beverages. Some parents even use their children as objects of sharing, and post about their children continuously. Parents who use social media share important moments before and after their children’s birth on their accounts. This is known as “sharenting.” “Sharenting” is when parents, caregivers, or relatives share content about their underage children on the Internet, including social media platforms such as Instagram, Facebook, and Twitter (Keskin, Kaytez, Damar, Elibol, & Aral, 2023, p. 2). Parent’s desire to be the center of attention has contributed to the rise of the “sharenting” phenomenon. This syndrome can lead to the emotional neglect and abuse of children as parents may prioritize the creation of content to engage their followers instead of the needs of their child. The higher digital skill of parents the greater possibility of engaging in “sharenting” behaviors and is strongly associated with technology-based addictions.

“This study was designed with a survey model among quantitative research methods. Data were collected through social network sites with snowball sampling method. The sample consisted of people aged 18 years and over from Turkey (n = 427).” (Keskin, Kaytez, Damar, Elibol, & Aral, 2023, p. 1) A total of 86.9% of the participants stated that sharing children’s photos and videos on social media platforms by parents, relatives and caregivers can be evaluated as child neglect and abuse. The variables of ‘gender’ and ‘the impact of sharing on children’ are factors that are associated with determining whether the sharenting syndrome is classified as abuse or not. Gender is a negative predictor of the classification of sharenting on social media as a type of child abuse and neglect. Since the use of social media by people is increasing, there should be measures to protect children from sharenting syndrome” (Keskin, Kaytez, Damar, Aral, 2023).
Methods
This study distributed a survey online between July 2022 and September 2022. Over 400 individuals, mostly female, over the age of 18 years completed the survey voluntarily. A third of participants reported having more than one social media account. Two-thirds of participants reported having children.

Takeaways
Children whose parents share their pictures on social media start having a digital footprint that follows them into adulthood before they even start walking. As these children enter adolescence, they reported being embarrassed by and disapproving of their parent’s sharenting posts. However, there are positive and negative associations with “sharenting.”

Positive Aspects
On the positive side, parents can support each other and share their experiences. Of the participating 385 parents in a quantitative survey model study with expert opinion, 72 percent reported that sharenting through social media is useful because it helps parents feel like they aren’t alone in their challenges.

Negative Aspects
Parents may unintentionally expose their children to risks while participating in sharenting. These risks include but are not limited to identify theft and use of children’s images on porn websites. Half of the photos shared by child sexual abusers were first posted on social media by parents as reported by the National Centre for Missing and Exploited Children (Keskin, Kaytez, Damar, Elibol, & Aral, 2023, p. 3). Also, comments on posts including children can affect their self-esteem.

Among posts, researchers found the following:
- 23.4% included ads
- 13.9% contained location
- 10.4% had children’s names
- 7.1% included educational and developmental material
- 5% contained embarrassing or private content

Summary 5
Children’s Online Safety: Predictive Factors of Cyberbullying and Online Grooming Involvement


Abstract
“The increase in the use of the Internet, strongly boosted by the spread of COVID-19, has amplified the risk of involvement in cyberbullying and online grooming among minors. To date, most research on these phenomena has focused on middle and high school students, with fewer studies on younger children. The present study aims to fill this knowledge gap by measuring the spread of cyberbullying and online grooming in a sample of 410 primary school students in the city of Rome and by identifying the main individual and environmental predictors associated with the involvement of children in these phenomena using factor analysis. Results indicate that both cyberbullying and online grooming are widespread among respondents, showing common traits within the four latent dimensions identified. Screen time is among the main predictors of children’s involvement, together with parental supervision, phubbing behaviours, prosocial tendencies and family socio-economic background. These findings highlight the need for further studies on representative samples of this age group, as well as for a greater cooperative effort among schools, parents and caregivers to keep children safe in the virtual world” (Tintori, Ciancimino, Bombelli, De Rocchi, & Cerbara, 2023).

Background
The research article delves into the issue of online grooming among elementary-school-aged children in Rome, focusing on the context of increased online activity prompted by the COVID-19 pandemic. Notably, the article highlights the concerning rise in Internet usage among children aged 6 to 10. For instance, between 2019 and 2021, use of the Internet among elementary-aged minors increased from 62.5% to 89.1%, according to the National Institute of Statistics (pg. 1). While discussions about bullying and online grooming have primarily centered on older minors, this study spotlights their prevalence among younger children. It is worth noting for this summary that online grooming is defined as the manipulative process by which adult strangers establish emotional connections with minors through online platforms, with the ulterior motive of engaging in sexual abuse or exploitation (pg. 3).

Methods
To investigate online grooming among this young age group, researchers undertook a survey in Rome, encompassing elementary school children across eight schools. The survey was conducted over the span of April to May 2021 and covered topics such as online grooming, bullying experiences, screen time habits, friendship dynamics, emotional well-being, and essential demographic information. A notable cohort of 410 children participated in the survey, with the gender distribution consisting of 53.7% male and 46.3% female respondents. The central objective of the research was to illuminate the nuanced impacts of various factors, including screen time, socio-economic backgrounds, social context, and parental supervision, on children’s susceptibility to online grooming.

Takeaways
Researchers’ analysis of the data underscores the prevalence of online grooming and perpetration among elementary-school-aged minors. The data highlights two distinct groups at a higher risk of exposure: (1) older children whose parents exhibit low levels of education and
employment status, and (2) children with limited parental oversight over their online activities. Interestingly, socio-economic status does not predict exposure to online grooming. However, the participant’s emotional well-being and discomfort were high risk factors for online grooming.

Ultimately, “the time spent in front of a screen, both on videogames and social media and [apps], is the main predictor for the involvement of kids in online grooming” (pg. 14). For instance, over half of participants reported at least a “medium” level of screen time on video games regularly (pg. 8). Meanwhile, nearly one in five participants reported a high level of screen time on social media (pg. 8) These responses correlated with risk of online bullying, leading to poorer emotional well-being for elementary-school-aged participants.

This research article examines the presence of online grooming among elementary-school-aged children in Rome, especially given increased use of the Internet and online tools since COVID-19. The study underscores parental supervision, emotional well-being, and the regulation of screen time as key mitigators against online grooming and bullying for this specific age group.


---

**Summary 6**

**A Critical Analysis of Fraud Cases on the Internet**


**Abstract**

We lived in the era of technology, where online websites have made communication and interaction much easier than the early decade. The modern world is changing so quickly, and emerging new trends simplify our lives, but on the other hand, it will also create risks. A website acts as a more admired platform by the user to access the different web applications. Because of the functions of the website, all the data on the website is available in the proper structure, which makes the working environment much more convenient and efficient. The websites may undoubtedly be a precious resource for young people, but it may also cause severe problems. It is really easy to build a fake website that looks like an original website where hackers like to deceive consumers and businesses for their own benefits. In this paper, researchers have examined online fraud cases through web applications and how fraudulent websites affect financial loss. Researchers also highlighted the current situation regarding the usage of online services, as well as the threats that have an impact on users. In addition, researchers have suggested that new
laws and regulations will be implemented for preventing cybercrime.

Background
Online web use has skyrocketed within the last decade. Users on the Internet have doubled from 2009 to 2019 (1), and there are more than 1.5 billion different websites on the World Wide Web today. From data transfer to online banking, the sharing of personal and financial information on the web has become increasingly prevalent on the web. However, as popularity on the web continues to rise, so do the various online scamming tricks that frauds use to extract user information and breach data protection security. This study aims to report the extent to which fraud has plagued the Internet and raise awareness on the need for websites to protect individual data.

Methods
The study analyzes different types of the number of fraud cases, scams, phishing cases, etc. in India over the past few years, recorded annually.

Takeaways
**Online scams have continued to grow with the increased use of online activity by users.** The number of reports from online shopping scams in India have skyrocketed from 9,953 cases in 2019 to 15,307 in 2020, with losses increasing from $4,845,452 to $8,428,525 (2173). Threat and extortion scams that hijack software and use malware to threaten job, life, etc. have also grown from around 15,000 cases in 2019 to over 35,000 in 2020, with financial losses tripling from around $40 million to nearly $120 million (2177).

Victim support services in India are mainly focused on physical/violent crime instead of financial damages, highlighting a lack of assistance for customers who suffer from online scams. The study also highlights a lack of a fast-rapid court system in dealing with online scams. They call for a need of a provision for fraud victims to file their complaints to the police, and an entirely new court in a separate cell so that they can be brought to justice (2184).

Summary 7
How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails


Abstract
“This empirical study is an exploration of the influence methods, fear appeals, and urgency cues applied by phishers to trick or coerce users to follow instructions presented in coronavirus-themed phishing emails. To that end, a content analysis of 208 coronavirus-themed phishing emails has been conducted. We identified nine types of phishing messages crafted by phishers. Phishing emails purporting to provide information about the spread of the disease were the most common type of unsolicited emails. Authority, liking and commitment emerged as the most common influence methods. Fear appeals and urgency cues were present in almost all of the sampled phishing messages. Finally, the analysis of coronavirus-themed phishing emails revealed a shift in the modus operandi of phishers. The implications of these results are discussed in this paper.”

Background
The arrival of the COVID-19 pandemic has given way to a sudden surge in COVID-19 related urgency emails, websites, and other related domains, caused by rising user demand for information about the extent of the pandemic’s spread and different protection methods. Many of these new domains are actually malware or phishing scams in disguise, and previous studies have reported a significant rise in online fraud since the beginning of the epidemic. The transitioning of society towards working and doing activities online more frequently, combined with greater levels of mental anxiety due to the lack of interpersonal communication from the pandemic, puts individuals at greater risk of falling victim to various ploys of online phishing. This study seeks to uncover the “modus operandi”, or the particular methods, that online perpetrators use to send phishing scams in order to better educate the public and protect themselves from them.

Methods
The study initially retrieved 2,372 images of various phishing emails from April 1st to April 16th, 2020, during which information about the disease was the most limited and individuals were most eager to search online to retrieve it. They were found from official sources such as Action Fraud or the Federal Bureau of Investigation. They then narrowed them down to 208 unique emails to eliminate redundancy, and used them for the final analysis, although the study also states that they mainly focused on 40 emails that were particularly heavy with information (Akdemir 3). The study performed a two-part analysis on these emails; The first part examined what type of content each email contained, the second part examined what types of social engineering methods were used in the email to lure its recipients into their scam. An approach known as the Qualitative Content Analysis (QCD) method was used, where the text of the email is reduced into its basic terms and is then systematically classified into different categories, sorting them by “research findings” and “influence methods” (5-6).

Takeaways
The results found that the most popular themes of online phishing email content contained content that “pretended to offer solutions to prevent the spread of the coronavirus outbreak” that asked users to download malicious attachments, with 23 emails, followed by those offering “financial
“benefits” that tricked users into entering personal information, at five emails, and those that ask for donations towards nonprofit organizations fighting the pandemic, at three emails (Akdemir 7). The second part of the analysis, examining social engineering methods, revealed that authority (asking the user to obey an order required from a higher-up, like a company or government) was the most common method of persuasion in the emails, at 23 emails, followed by commitment (requesting the user to perform an action that “they have done before”), at 13 emails, and liking (thanking the user and appreciating their time), at 7 emails (Akdemir 8). Finally, the study also noted a linkage between emails that offered “information and solutions” to the virus and emails that used authoritative methods of social engineering, stating that 19 out of 23 information-providing emails used authoritative language in their phrasing (Akdemir 8).

The study’s results demonstrate how quickly phishers have taken advantage of the sudden change in climate from the COVID pandemic, developing 23 different email formats pretending to offer information about the pandemic to users during a period when the pandemic was at its very early stages.

The study also notes that the “modus operandi” of delivering the scams has shifted from clicking links or buttons to downloading attached files and documents, which is significant because most phishing cases previously focused on providing financial support through malicious links. The study suggests that perpetrators will continue to couple malicious COVID-19 emails with attached, downloadable ransomware, and warns users to look out for emails that are structured in such a format.


Summary

Teachers’ Management of Cyberbullying on China’s Social Media Sites: A Case Study in Shandong Province, China


Abstract

“In recent years, cyberbullying on social media sites has increased among adolescents and even adults. While there are many factors and forms of cyberbullying, schoolchildren are vulnerable groups that are exposed to cyberbullying threats to their mental and emotional health. On the other hand, teachers have the responsibility in the place of the parent while at school, and they need to manage the issue at bay. This study focuses on the identification and analysis of teachers’ advice about cyberbullying, thus leading to the conceptualization of a decision-making model for the school to guide other teachers on this matter...”
Background
Cyberbullying has become a major problem worldwide thanks to the rise of technology and mobile devices becoming more prominent in day-to-day life. It is defined as the harassment and/or the act of threatening others on online social media platforms, and can have tremendous effects on mental and psychological health, especially on younger children. China has taken cyberbullying very seriously, declaring it a “national threat” nationwide, with its president Xi Jinping announcing a 1 billion-yuan campaign towards helping children avoid cyberbullies. School administrations have also been encouraged to take initiative at combating the issue. This study suggests looking at how teachers across China have dealt with cyberbullying incidents in order to obtain a better framework at dealing with them. The goals of the study are organized into two parts: To gather data on how teachers help students avoid and deal with cyberbullying confrontations, and use that data to propose a suitable decision-making model that can be implemented in schools across the nation.

Methods
The study chose one specific school to investigate, a semi-private school in the region of Shandong, China, that serves 410 teachers and over 6,000 students (5). Thirty-two teachers volunteered to participate in the study. The data was collected via an online survey, with teachers being asked to type their response to an open-ended question: “What was your best advice given to the student victims of cyberbullying?”

Takeaways
This study emphasizes the crucial role that teachers play in preventing, dealing with, and helping students who have suffered from cyberbullying incidents. The advice and knowledge they give towards cyberbullying are valuable sources of information for schools and policymakers to decide what steps to take towards cyberbullying and other sources of mental health problems in China. Teachers that responded to the survey question gave advice that were mainly split into three categories: Preventative measures (Methods to prevent cyberbullying from occurring in the first place), counteractive measures (What to do when involved in a cyberbullying incident), and corrective measures (Ways to seek help and recuperate after experiencing a cyberbullying incident).
The study contains a flow chart that lists out preventive, counteractive, and corrective measures that were stated by teachers in the event of cyberbullying. The different branches represent the different options that correspond to each type of measure. For this summary’s purposes, the information from those flow charts is outlined below:

1. Preventive Measures
   a. Control how much to share and post online
   b. Keep passwords and computer safe
   c. Think over message before posting
   d. Do not post any personal and private information
   e. Do not post grievances, without or without a person’s name
   f. Remind parents to monitor children’s activities

2. Counteractive Measures to Targeting by a Cyberbullying
   a. Do not react with an argumentative tone
   b. Stand up for yourself
   c. Block the potential bully
   d. Do not reply to anonymous/strangers’ messages
   e. Do not reply to the bully

3. Corrective Measures
   a. Do not try to resolve the issue alone
   b. Keep a record of all communications
   c. Encourage children and adults to talk to someone
   d. Know where to report cyberbullies