

## PSYCHOLOGICAL IMPACT OF CYBERCRIMES – AN OVERVIEW

**Dr. Theju Kumar C**

Assistant Professor & Head, Department of Criminology, Acharya Institute of Graduate Studies, Bengaluru – 560 107, Karnataka, India

**Abstract** - Psychological science of criminal behavior from a unique perspective. The web brings with it new crimes and new ways in which to commit previous crimes, and has the potential to create a criminal of the unsuspecting and naïve net user. This chapter introduces the reader to the realm of cyberpsychology and provides an outline of current psychological understandings of on-line crime. We tend to begin by considering crime typologies, outlining the classes of cybertrespass, cyberdeception and stealing, cyber-pornography and obscenity, and cyber-violence that have enlightened psychological theorizing during this space, likewise as highlight a number of the issues inherent among these categorization systems. We tend to then specialise in the psychological science of exploitation the web as a tool for brand new and previous crimes, wherever a wrongdoer might use the web as a “weapon” that has the potential to cause damage or harm. Here, we tend to specialise in the previous crime of domestic abuse that's committed through the new technology of the web and therefore the associated new crime of revenge porno that depends on the web and joined technologies to cause harm to its victims. We tend to end by considering a number of the difficulties of researching on-line crime from a psychological perspective and propose a requirement for psychological theorizing to manoeuvre removed from categorizing massive sways of gently connected crimes below umbrella labels. With this backdrop the present paper made an attempt to explain the psychological impact of cybercrimes and its various aspects.

**Key Words:** Cyber Crime, Cybersecurity, Psychological Change, Cybercrime, Criminals

### INTRODUCTION

Cybercrime is any criminal act related to computers and networks which is called hacking, phishing, spamming, or is used as a tool to commit an offense conducted through the Internet. It is a bigger risk now than ever before due to the sheer number of connected people and devices. Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission. Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who are engaged in these illegal activities are often referred to as hackers. Common types of cybercrime include online bank information theft, identity theft, online predatory crimes, and unauthorized computer access. More serious crimes like cyber-

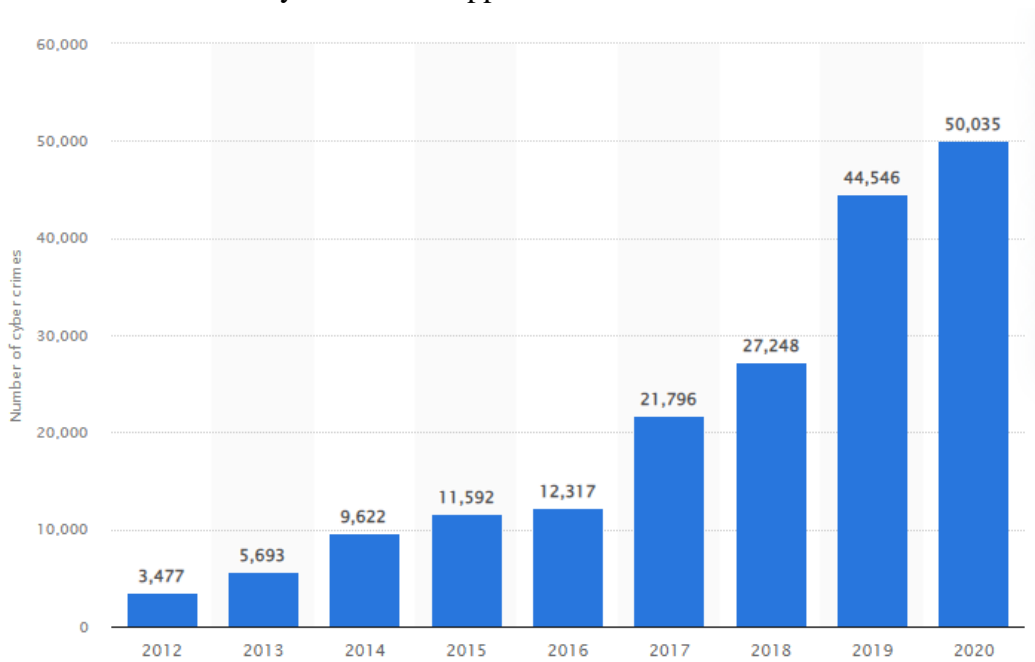
terrorism are also of significant concern. Cybercrimes cover a wide range of activities, but these can generally be broken into two categories, crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks, and crimes that use computer networks to advance other criminal activities. These types of crimes include cyber-stalking, phishing, fraud, or identity theft. Criminals committing cybercrime use a number of methods, depending on their skill-set and their goal. Cybercrime, as distinguished from computer crime, is an umbrella term for various crimes committed using the World Wide Web, such as, theft of one's personal identity or financial resources, spread of malicious software code such as computer viruses; use of others' computers to send spam email messages, Denial of Service (DoS) attacks on computer networks or websites by the hacker, activism, or attacking computer servers of those organisations felt by the hacker to be unsavoury or ethically dubious, cyberstalking by which sexual predators use Internet chat rooms, social networking sites, and other online venues to find and harass their victims, cyberbullying, where individuals are harassed by others, causing severe mental anguish, cyber pornography, the use of the Internet to spread child and adult pornography; Internet gambling and software piracy and cyber terrorism, the use of the Internet to stage intentional, wide-spread attacks that disrupt computer networks, using the Internet to spread violent messages, recruit terrorists, and plan attacks. Cybercrime can be divided into four sub-categories cyber-trespass, cyber-deceptions, cyber-pornography, cyber-violence, the facilitator of the crime, or the target of the crime.

#### **NUMBER OF CYBERCRIMES IN INDIA**

National Crime Records Bureau (NCRB) report quantifies for the primary time the bizarre trends in crime and law and order in a very year once a lot of of the country was in a very imprisonment for over 2 months. Crime sections embrace many forms of crimes that square measure either dole out victimization or primarily target laptop systems or assets connected to the web, like net banking and email accounts. Bharat recorded fifty, 035 cases of crime in 2020, with an 11.8% surge in such offenses over the previous year, as 578 incidents of "fake news on social media" were additionally reported, official knowledge showed on Sept fifteen. The speed of crime incidents per 100000 populations additionally rose from three.3% in 2019 to three.7% in 2020 within the country, per the National Crime Records Bureau (NCRB) knowledge. In 2019, the country recorded forty four, 735 cases of crime, whereas the figures stood at twenty seven, 248 in 2018, the information from corresponding years showed. The year saw four,047 cases of on-line banking fraud, 1,093 OTP frauds, and 1,194 credit/debit card fraud, while 2,160 cases associated with ATM were reported in 2020, the NCRB figures showed. There have been additionally 578 cases of faux news on social media, 972 associated with cyber stalking or bullying of ladies and youngsters, 149 incidents of faux profiles and ninety eight of information thievery, it added. In terms of motive, the most sixty.2% cyber crimes lodged in 2020 were in deep trouble fraud (30,142 out of fifty, 035 cases), the NCRB, that functions beneath the Ministry of Home Affairs, stated. it had been followed by sexual exploitation with six.6% (3,293 cases) and extortion four.9% (2,440 cases), the information showed. Among States, the most of eleven, 097 crime cases was reported in Uttar Pradesh followed by state (10,741), geographical region (5,496), Telangana (5,024), and state (3,530),

it showed. However, the rate was highest in state with sixteen.2 % followed by Telangana (13.4%), Assam (10.1%), Uttar Pradesh (4.8%), and geographical region (4.4%), the information showed. city metropolis recorded 168 such cases throughout the year with a criminal offense rate of zero.8%, per the NCRB, that is to blame for aggregation and analyzing crime knowledge as outlined by the Indian legal code and special and native laws within the country. Figure one depicts the whole variety of cybercrimes that happened in Bharat from 2012 to 2020.

Figure 1. Total Number of Cybercrimes Happened in India from 2012 to 2020



*Source:* www.statista.com

## THE PSYCHOLOGICAL IMPACT OF CYBERCRIME

Cyber-attacks/scams are available several forms; from romance scams, to phishing attacks, ransomware attacks and additional. Reports of economic, employment or information losses or alternative kinds of losses, like personal information, are often not solely important however devastating. The data typically will be taken and distributed therefore apace those intense feelings of helplessness and impotency square measure often skilled. Victims usually have the out of management feeling, in turn, resulting in additional anxiety and feeling discouraged. The emotional and psychological impact following the losses associated with crime will vary from gentle to severe and cause symptoms of depression, anxiety, panic attacks, posttraumatic stress and even suicide. The psychological state conditions square measure more exacerbated by varied psychosocial losses associated with finances, employment, family and/or relationships. a brand new study by Norton reveals the staggering prevalence of cybercrime: sixty fifth of net users globally, and seventy three of U.S. internet surfers have fallen victim to cybercrimes, together with laptop viruses, on-line MasterCard

fraud and fraud. Because the most ill-used nations, America ranks third, once China (83%) and Brazil and Republic of India (76%).

The first study to look at the emotional impact of crime, it shows that victims' strongest reactions square measure feeling angry (58%), irritated (51%) and cheated (40%), and in several cases, they blame themselves for being attacked. solely three-d don't assume it'll happen to them, and nearly eightieth don't expect cybercriminals to be dropped at justice leading to an ironic reluctance to require action and a way of helplessness. Despite the emotional burden, the universal threat, and incidents of crime, individuals still aren't dynamic their behaviors with solely 0.5 (51%) of adults spoken language they'd amendment their behavior if they became a victim. Even scarier, less than 0.5 (44%) reportable the crime to the police.

Cybercrime victim Todd jurist of Chicago explained, "I was showing emotion and financially unprepared as a result of I ne'er thought I might be a victim of such against the law. I felt profaned, as if somebody had truly returned within my home to assemble this data, and as if my entire family was exposed to the current criminal act. Currently I can't facilitate however marvel if alternative data has been lawlessly non-heritable and simply sitting within the wrong people's hands, anticipating a chance to be used. Determination crimes are often extremely frustrating: in line with the report, it takes a mean of twenty eight days to resolve a crime, and therefore the price to resolve that crime is \$334. Twenty-eight pc of respondents same the most important problem they featured once managing crime was the time it took to unravel.

But despite the trouble, coverage a crime is essential. All obtain crime, either directly or through pass-along prices from our monetary establishments, same Adam Arnold Palmer, Norton led cyber security authority. Cybercriminals by choice steal tiny amounts to stay unobserved, however all of those add up. If you fail to report a loss, you'll truly be serving to the criminal keep beneath the measuring instrument. The human impact facet of the report delves more into the limited crimes or white lies shoppers commit against friends, family, beloved ones and businesses. Nearly 1/2 respondents assume it's legal to transfer one music track, album or moving-picture show while not paying. Its legal or dead okay to in secret read somebody else's e-mails or browser history. A number of these behaviors, like downloading files, open individuals up to further security threats. The invasion to one's privacy that results from cyber-attacks conjointly interprets into grief.

### ***Grief that Results From Cybercrime***

The losses that result from cyber-attack further because the invasion of one's privacy all translate into grief. A grief that's not solely felt through mixed emotions like denial, anger, depression, and anxiety however through the loss of the sense of self and to one's role and identity. Grief is additionally felt through the loss within the kind of distrust in oneself and distrust of others. The self will feel shattered. The emotional, cognitive, behavioural, and physical symptoms of falling victim to law-breaking embrace the followings:

The emotional symptoms will embrace feeling depressed, sad, anxious, guilty, ashamed, disheartened, and angry. Common feelings may embrace feeling betrayed, powerless, out of management, and vulnerable. The psychological feature symptoms will embrace a negative appraisal of self, perceiving the self as a failure or weak; reduced shallowness and self-confidence; problem focusing or feeling scattered. Raised worry and negativity; concern for safety and feeling unsafe. The behavioural symptoms will embrace isolation; withdrawal; reduced interest in activities; increase in substance misuse like medicine, caffeine, nicotine, or unhealthy coping; raised food for comfort, problem falling or staying asleep or early morning awakening; and/or appetency changes. The physical symptoms will embrace headaches; muscle tension; aches; abdominal distress; intake a lot of or less and sleeping a lot of or less.

### ***Prevention at Each Structure and Individual Levels***

Firstly, organizations have to be compelled to properly educate and train their workers on the way to spot and stop numerous forms of cyber-attacks. Often conducted cyber user awareness coaching bestowed and practiced in an open and honest manner helps to organize workers from recognizing these forms of frauds. Organizations have to be compelled to inform workers on an everyday basis further as once new cyber-attacks become familiar and steps on the way to proceed if they witness or receive an uncommon demand or activity. Recurrent education around consulting 1st before responding or clicking AN email or gap a hooked up document must be provided on an everyday incidence. However, if a worker will click on a malicious link, or follow the directions in a very well-crafted phishing email, the organization should take away the shaming mentality that a lot of have if somebody will accidentally do one thing that puts the corporate in risk. we've got detected several stories from organizations during which their workers didn't tell anyone once they clicked on an attachment as a result of they were embarrassed, guilty, or were afraid. It had been someday later once the geographical point systems were utterly encrypted with Ransomware that the employees' actions were familiar. We tend to all build mistakes, and criminals square measure creating it extremely arduous to tell apart what's real and what's pretend. We want to encourage our workers to let somebody recognize as shortly as attainable if they suppose they've done one thing wrong. Organizations should notice that in these difficult times individuals square measure fagged and distracted, creating them straightforward targets for cybercriminals. Organizations ought to encourage their workers to "slow things down a little" and take a flash or to essentially check up on an email to see if it'd be phishing for info or asking them to follow directions. At the Individual level, here square measure some healthy brick ways within the aftermath of cybercrime:

Identify however you are feeling and your thoughts. Notice there square measure traditional reactions which you're not alone. Prompt yourself of your positives, qualities, and achievements despite the loss-related law-breaking and the way you are felt betrayed or robbed. Follow self-care by catching reframing your thoughts and equalization them; participating in a very diet and regular exercise; correct sleep hygiene; and setting meaty activities. Avoid self-blaming. Place it slow and energy into what you've got management over, and use what you've got learned constructively to raised shield yourself. Gather correct

support, resources, and services to make sure your safety and scale back the chance of being re-victimized. follow self-compassion by being kind to yourself, not deciding yourself, being conscious of your thoughts and feelings, putt them into perspective; acknowledging and acceptive that you just square measure a personality's being, and acceptive the imperfections that go with being human. Avoid substance misuse or any unhealthy brick. Get social support. You may realize it useful to affix support teams for victims of law-breaking or any victim support teams. don't hesitate to hunt skilled facilitate if you're experiencing increasing psychological distress; problem initiating tasks or taking care of responsibilities; inveterately depressed mood, or excessive anxiety that's more and more tough to manage; lacking pleasure in activities; difficulties with sleep and/or concentration; or different psychological symptoms which may as a result of you concern.

### **PSYCHOLOGICAL IMPACT OF CYBERCRIME LEADS STRESS**

In 2015, hackers targeted a web site for those collaborating in extra-marital affairs. The info from over cardinal million Ashley Madison web site users was leaked. Four victims committed suicide, one from the threat of exposure. This can be a stark example of the growing drawback that leaves victims grappling with the way to handle the emotional value of crime from the invasion of privacy to worry of monetary ruin. Within the case of the Ashley Madison web site, the target wasn't cash. The goal was to shut the location down. The cluster taking responsibility for the hack known as activists, WHO attack a cause by mistreatment hacking as a tool. Still, the crime was even as hurtful to its victims. Consistent with a recent study, the emotional impact of crime is commonly relative to the quantity of cash lost compared to associate degree individual's internet value. a fashionable victim would feel less emotional distress concerning losing but one hundred pounds, than a unfortunate person. However, if a fashionable person lost a major quantity of his or her internet value, they'd probably expertise similar feelings of stress. Bound on-line scams need that the grafter build a relationship with the victim. Romance scams, advance fee fraud, and rental scams square measure a couple of samples of scams that need the fraudster to act with the victim to realize his or her trust before revealing it. These crimes square measure notably brutal on the victim, going away in its wake feelings of insecurity and devastation. The emotional manipulation is as well as money stealing, increasing the sense of loss.

### **STEPS TOWARD RECOVERY**

There square measure many ways in which to supply support to victims of on-line crime. Like the majority operating through trauma, having an addict to pay attention to is often useful and may relieve a number of the uneasiness. Emotional issues will last well when the scam is over. Healing takes time, thus don't decide. Some fortunate therapies involve dynamic the victim's perception by viewing the expertise as a lesson that helps in learning the way to higher shield his or her money and alternative interests. A victim could feel additional of associate degree emotional impact on the far side the stealing knowledge of information if personal or money data is employed. Facilitate to attenuate opportunities for repeat victimization by considering a credit freeze, dynamic the approach that you just act on-line, and keeping your pc secure with the newest updates and anti-virus package. Most Brits

won't be victims of crime, except for the little proportion that finds themselves experiencing the traumatic emotional roller coaster that accompanies these on-line breaches of trust, you'll recover. Take the necessary steps in emotional recovery by limiting possibilities for re-victimization. Keep proactive in protective your info. Be a champion for those whose lives are vertical by coverage suspected crime to the right authorities and posting fraud alerts on-line to assist others avoid this expertise.

## **RECOMMENDATIONS FOR STRENGTHENING CYBER SECURITY POLICIES**

McAfee and also the Digital agency security Forum (DGSF) discharged a brand new report that explores the cyber risks attempt the govt and offers recommendations to mitigate these risks. The report provides the outlines of 2 tools, a urged Review method, and a projected Development Framework to assist boards, senior managers, and information and knowledge groups in organizations that will wish to review their information security methods and governance arrangements. Since its launch in March this year, the DGSF actively engaged with civil servants, cyber specialists, and technology suppliers to assist guide the event of the Forum and to help in quality reassuring the work made through the initiative. The report identifies four high priority areas, for state to handle because it continues to form larger use of technology to satisfy asceticism targets and improve the delivery of digital public services: Lack of awareness of knowledge security threats at the board level, inflicting organizations to fail to supply support that they're meeting their info security responsibilities and cost-effectively managing info and cyber threats. Considerations over information security block efforts to spice up collaboration, information sharing, and additional economical performing at a time once government and public services square measure fraught to deliver additional at a lower value. Interfaces between totally different organizations square measure key danger points because the government's prime objective is to hitch up services and promote larger partnership operating and collaboration across sectors. Request systems that weren't designed for the digital age have inspired bequest thinking in terms of knowledge security, typically leading to fragmented and siloed security arrangements. John architect, secretary to the Digital agency security Forum says: "Overall, the united kingdom has created large progress in info handling and information security following the series of status breaches in recent years. There's but no area for self-satisfaction. Organizations got to suppose in terms of security-by-default to deliver digital-by-default and share info so as to counter cyber threats. Crime is international in nature associate degree a robust public-private partnership is crucial to make a setting wherever public sector organizations will work along for mutual profit."The DGSF's suggested the subsequent measures to avoid cybersecurity problems.

- Be responsive to your risks and place foundations into place: determine key risks, vulnerabilities, and important info assets; implement basic controls and proactively manage info risks.
- Embrace technology: make sure that the protection technology infrastructure includes comprehensive threat intelligence, risk, and activity analytics, and robust, resilient, and automatic threat protection.

- Use improved info security as AN enabler: Support and alter the savings, service developments, and potency enhancements the digital world offers once security barriers are removed.
- Develop a culture that embraces change: Share expertise and experience across the general public sector to spice up confidence from voters, businesses, and therefore the government itself into these digital systems.

## CONCLUSIONS

As on-line threats and cyber-attacks still permeate the net, it's essential that we tend to as a community develop a much better understanding of those problems and the way they'll impact our lives. As shown from the studies given, understanding what results in victimization on-line could be an advanced issue reckoning on psychological feature, social, or skill-related factors. What's clearly illustrated is that more analysis is required so as to rose perceive the impact on multiple aspects of life for victims of on-line crime still because the victims' desires and so develop policies during this space. Additionally, we want to rose assess the information and skills of enforcement and judiciary which could more impact the ways that such victims area unit supported.

## References:

1. Agnew, R. S. (1985). Neutralizing the impact of crime. *Criminal Justice and Behavior*, 12(2), 221–239.
2. Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, 9(1), 35–54.
3. Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., O'Carroll, E. (2015). A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, 11(4), 373–391.
4. Andrews, B., Brewin, C. R., Rose, S. (2003). Gender, social support, and PTSD in victims of violent crime. *Journal of Traumatic Stress*, 16(4), 421–427. <https://doi.org/10.1023/A:1024478305142>
5. Australian Bureau of Statistics. (2019). 2017-2018 National Crime Victimization Survey (Cat. No. 4530.0). <https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4530.0Main+Features332017-18?OpenDocument>
6. Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191–215. <https://doi.org/10.1037/0033-295x.84.2.191>
7. Bard, M., Sangrey, D. (1986). *The crime victim's book* (2nd ed.). Brunner/Mazel.
8. Barnett, O. W., Martinez, T. E., Keyson, M. (1996). The relationship between violence, social support, and self-blame in battered women. *Journal of Interpersonal Violence*, 11(2), 221–233. <https://doi.org/10.1177/088626096011002006>
9. Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology*, 12(1), 22–42. <https://doi.org/10.1177/1557085116654565>
10. Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology*, 12(1), 22–42. <https://doi.org/10.1177/1557085116654565>
11. Belk, R. W. (1988). Possessions and the extended self. *Journal of Consumer Research*, 15(2), 139. <https://doi.org/10.1086/209154>



12. Belk, R. W. (2013). Extended self in a digital world. *Journal of Consumer Research*, 40(3), 477–500. <https://doi.org/10.1086/671052>
13. Braun, V., Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
14. Braun, V., Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*.
15. Breakwell, G. M. (2006). Interviewing. In Breakwell, G. M., Hammond, S., Fife-Shaw, C., Smith, J. A. (Eds.), *Research methods in psychology* (3rd ed., pp. 230–242).
16. Broadhurst, R. (2017). Cybercrime in Australia. In Deckert, A, Sarre, R (Eds.), *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice* (pp. 221–235). Palgrave Macmillan.
17. Button, M., Lewis, C., Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, 27(1), 36–54.
18. Correia, S. G. (2019). Responding to victimisation in a digital world: A case study of fraud and computer misuse reported in Wales. *Crime Science*, 8(4), 1–12.
19. Draucker, C. B., Stern, P. N., Burgess, A. W., Campbell, J. C. (2000). Women's responses to sexual violence by male intimates. *Western Journal of Nursing Research*, 22(4), 385–406. <https://doi.org/10.1177/019394590002200403>
20. Fischer, C. T., Wertz, F. J. (1979). Empirical phenomenological analyses of being criminally victimized. *Duquesne Studies in Phenomenological Psychology*, 3, 135–158. <https://doi.org/10.5840/dspp1979314>
21. Frieze, I. H., Hymer, S., Greenberg, M. S. (1987). Describing the crime victim: Psychological reactions to victimization. *Professional Psychology Research and Practice*, 18(4), 299–315. <https://doi.org/10.1037/0735-7028.18.4.299>
22. Golladay, K., Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, 12(5), 741–760.
23. Green, D. L., Pomeroy, E. (2007a). Crime victimization: Assessing differences between violent and nonviolent experiences. *Victims & Offenders*, 2(1), 63–76. <https://doi.org/10.1080/15564880600922117>
24. Greenberg, M., Ruback, R., Westcott, D. (1983). Seeking help from the police: The victim's perspective. In Nadler, A., Fisher, J., DePaulo, B. (Eds.), *New directions in help: Vol. 3. Applied perspectives on help-seeking and-receiving* (pp. 71–103). Academic Press.
25. Henson, B., Reyns, B. W., Fisher, B. S. (2016). Cybercrime victimization. In Cuevas, C. A., Rennison, C. M. (Eds.), *The Wiley handbook on the psychology of violence* (pp. 553–570). John Wiley.
26. Janoff-Bulman, R. (1985). The aftermath of victimisation: Rebuilding shattered assumptions. In Figley, C. (Ed.), *Trauma and its wake* (Vol. 1, pp. 15–35). Brunner/Mazel.
27. Janoff-Bulman, R. (1985). The aftermath of victimization: Rebuilding shattered assumptions. In Figley, C. R. (Ed.), *Trauma and its wake* (pp. 15–35). Brunner/Mazel.
28. Jansen, J., Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91. <https://doi.org/10.5281/zenodo.58523>
29. Kunst, M. J. J., Rutten, S., Knijf, E. (2013). Satisfaction with the initial police response and development of posttraumatic stress disorder symptoms in victims of domestic burglary. *Journal of Traumatic Stress*, 26(1), 111–118.

30. Kunst, M. J., Koster, N. N. (2017). Psychological distress following crime victimization: An exploratory study from an agency perspective. *Stress and Health*, 33(4), 405–414. <https://doi.org/10.1002/smi.2725>
31. Liamputtong, P. (2009). Qualitative data analysis: Conceptual and practical considerations. *Health Promotion Journal of Australia*, 20(2), 133–139. <https://doi.org/10.1071/HE09133>
32. Norris, F. H., Kaniasty, K. (1994). Psychological distress following criminal victimization in the general population: Cross-sectional, longitudinal, and prospective analyses. *Journal of Consulting and Clinical Psychology*, 62(1), 111–123. <https://doi.org/10.1037//0022-006x.62.1.111>
33. Pietkiewicz, I., Smith, J. (2014). A practical guide to using interpretative phenomenological analysis in qualitative research psychology. *Czasopismo Psychologiczne: Psychological Journal*, 20(1), 7–14. <https://doi.org/10.14691/cppj.20.1.7>
34. Sebele-Mpofu, F. Y., Serpa, S. (2020). Saturation controversy in qualitative research: Complexities and underlying assumptions. A literature review. *Cogent Social Sciences*, 6, 1. <https://doi.org/10.1080/23311886.2020.1838706>
35. Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., Hutton, S. (2003). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences*, 49(1), 131–136. <https://doi.org/10.1520/JFS2003178>
36. Van der Wagen, W., Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, 17(4), 480–497.
37. Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry Psychology and Law*, 24(3), 323–338. <https://doi.org/10.1080/13218719.2017.1315785>
38. Worsley, J. D., Wheatcroft, J. M., Short, E., Corcoran, R. (2017). Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. *Sage Open*, 7(2), 1–13. <https://doi.org/10.1177/2158244017710292>