Current Psychiatry Reports (2021) 23: 18
https://doi.org/10.1007/s11920-021-01228-w

PSYCHIATRY IN THE DIGITAL AGE (J SHORE, SECTION EDITOR)

Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry

Scott Monteith[1] · Michael Bauer[2] · Martin Alda[3] · John Geddes[4] · Peter C Whybrow[5] · Tasha Glenn[6]

Accepted: 21 January 2021 / Published online: 3 March 2021

Abstract

Purpose of Review Since the pandemic, the daily activities of many people occur at home. People connect to the Internet for work, school, shopping, entertainment, and doctor visits, including psychiatrists. Concurrently, cybercrime has surged worldwide. This narrative review examines the changing use of technology, societal impacts of the pandemic, how cybercrime is evolving, individual vulnerabilities to cybercrime, and special concerns for those with mental illness.

Recent Findings Human factors are a central component of cybersecurity as individual behaviors, personality traits, online activities, and attitudes to technology impact vulnerability. Mental illness may increase vulnerability to cybercrime. The risks of cybercrime should be recognized as victims experience long-term psychological and financial consequences. Patients with mental illness may not be aware of the dangers of cybercrime, of risky online behaviors, or the measures to mitigate risk.

Summary Technology provides powerful tools for psychiatry but technology must be used with the appropriate safety measures. Psychiatrists should be aware of the potential aftermath of cybercrime on mental health, and the increased patient risk since the pandemic, including from online mental health services. As a first step to increase patient awareness of cybercrime, psychiatrists should provide a recommended list of trusted sources that educate consumers on cybersecurity.

Keywords Cybercrime · Psychiatry · Pandemic · Human-computer interface · Cybersecurity

Introduction

The pandemic has profoundly changed how people use technology. For a large number of people, routine daily activities now occur at home using a connection to the Internet, including work, school, shopping, doctor visits and entertainment. As time spent online has increased, cybercrime has grown dramatically. This is of concern to psychiatry since the human dimension is a fundamental aspect of cybersecurity [1–3]. The surge in cybercrime was noted in a joint alert from security officials in the USA and UK [4], and a report from Interpol [5]. The FBI stated that the number of cybercrime complaints in between January through end of May 2020 were nearly the same as for the entire year of 2019 [6]. Cybercrime has wide-ranging, long-lasting effects across society, targeting individuals, small and large businesses, academia and governments. Even before the pandemic, cybercrime was recognized as a major global risk [7]. In 2018, it was estimated in that cybercrime cost the world $600 billion, and that two billion people have had personal data stolen or compromised [8].

Technology provides powerful tools, but like any tool, may be dangerous if not used with appropriate safety measures. The challenge of dealing with cybercrime is complex. Human factors and the human-computer interface are a central component of cybersecurity, and technology alone will not prevent cybercrime [1–3]. Susceptibility to online fraud is associated with an individual's behaviors and personality traits [9, 10], and mental illness may increase this vulnerability

This article is part of the Topical Collection on *Psychiatry in the Digital Age*

✉ Scott Monteith
monteit2@msu.edu

[1] Michigan State University College of Human Medicine, Traverse City Campus, 1400 Medical Campus Drive, Traverse City, MI 49684, USA

[2] Department of Psychiatry and Psychotherapy, University Hospital Carl Gustav Carus Medical Faculty, Technische Universität Dresden, Dresden, Germany

[3] Department of Psychiatry, Dalhousie University, Halifax, Nova Scotia, Canada

[4] Department of Psychiatry, Warneford Hospital, University of Oxford, Oxford, UK

[5] Department of Psychiatry and Biobehavioral Sciences, Semel Institute for Neuroscience and Human Behavior, University of California Los Angeles (UCLA), Los Angeles, CA, USA

[6] ChronoRecord Association, Fullerton, CA, USA

[11]. The purpose of this narrative review is to discuss why the rapid growth of cybercrime is important to psychiatry. The topics include the changing use of technology, societal impacts of the pandemic, evolving cybercrime including medically related fraud, individual vulnerabilities, aftermath of cybercrime on mental health, special concerns with mental illness, and the need to educate physicians and patients.

Changing Use of Technology

Since the pandemic, people routinely use the Internet to work, study, shop, visit the doctor, entertain and access government programs. As a result, the demand for broadband communications services has soared globally, with some fixed and mobile operators reporting a 60% increase in Internet traffic [12]. For example, in the USA between 3/1/2020 and 6/26/2020, there was a downstream peak traffic growth of 20.1%, and upstream peak traffic growth of 36.9% [13]. The digital workplace and classroom at home have also changed the type of technology that people purchase and use. In 2020, smartphone sales declined globally by 20% in the first and second quarters [14, 15], and a decrease in the addition of new IoT (Internet of things) connections of 45% is estimated [16]. In contrast, shipments of the traditional PC market (laptops, desktops, notebooks) grew by 11.2% in the second quarter [17]. Other Internet habits have also changed since the pandemic. About 30% of people in the USA have increased their use of social media [18, 19]. Online shopping has increased globally, including in USA, UK, and Europe [20], and accelerated the use of digital alternatives to cash [21, 22].

There was an unprecedented increase in telemedicine since the pandemic across all specialties, but particularly in psychiatry [23, 24]. Psychiatry is well suited for telemedicine as most services do not require in-person interaction [23]. Many outpatients now routinely receive psychiatric care by virtual visits [25–27], and most expect telepsychiatry to be further optimized and persist indefinitely [23, 28].

Societal Impacts of the Pandemic

The pandemic has impacted communities everywhere. It is estimated that globally, 150 million people will be pushed into extreme poverty by 2021, with 8 out of 10 new poor living in middle-income countries [29]. In the USA, at least half of households have serious financial problems, including income loss, unemployment and trouble paying bills [30]. The financial distress is disproportionately high in minority, low income, and low education households [30, 31], and households with children under age 18 [32, 33]. Another change in the USA is that a majority of those aged 18–29 live with their parents for the first time since the Great Depression [34].

The isolation, disruption of daily routines, financial hardship, uncertainties, and frequent misinformation associated with the pandemic often has psychological impacts [35] with global reports of depression, anxiety, stress and loneliness in the general public [36–39]. Severe financial stressors may be associated with an increase in suicide attempts [40, 41]. A history of mental health problems increases the risk of the psychological impacts of the pandemic [42] in both adolescents [43, 44] and adults [39, 45–47]. People with a history of anxiety or mood disorders experience more severe pandemic-related fears [48], and those with mental problems frequently report insomnia [44, 46, 47]. Pandemic-related stress may increase alcohol and substance use [38, 49, 50].

Many people are avoiding getting healthcare during the pandemic. Nearly half of adults in the USA are concerned about catching the virus in medical settings including hospitals, outpatient clinics and laboratories, and have deferred medical care [51, 52] including those with mental illness [53, 54]. Some patients with mental illness may no longer be able to afford their medications [55]. A lack of regular treatment may increase the risk of psychiatric symptoms in those with severe mental illness [53]. Despite the increase in psychological stressors from the pandemic, emergency room visits for psychiatric problems have decreased in the USA and Europe [56–58].

Cybercrime Is Evolving

There is no reason to think cybercrime will decrease after the pandemic ends. Cybercrime has evolved from a nefarious hobby of individual hackers to a highly organized, international business network covering every aspect of cyberattack activities, including black markets for stolen data [59, 60]. With the widespread adoption of the cybercrime-as-a-service model, a broad range of attack "services" can be purchased through cybercrime markets on the dark web or hacker forums, with little technical expertise needed [59]. Traditional physical crime to steal money like breaking into a house or business leaves considerable evidence including DNA, fingerprints, shoeprints, and security camera recordings [61]. In contrast, a cybercriminal obscures their identity and has a very low risk of getting arrested or going to jail [8, 61].

Cybercriminals are maximizing the new opportunities related to the rapid increase in working from home and pandemic-related fears by emphasizing attacks that exploit human vulnerabilities [62]. Today's organized cybercriminals take advantage of the latest software and hardware developments just like legitimate developers. For example, cybercriminals may use machine learning to generate disinformation including text, fake image, video and voice, or to break CAPTCHA [63, 64]. Types of cybercrime that are frequently aimed at individuals are shown in Table 1. Of particular concern is the sharp rise in medical cybercrime triggered by the pandemic occurring worldwide [66]. Between February and March 2020, over 116,000 coronavirus themed new domain names were

Table 1 Some types of cybercrime that impact individuals

Type of cybercrime	Description [65•]
Phishing	Messages sent by email, social media, text messaging, or voice designed to trick users into divulging sensitive personal information (such as passwords, credit card numbers, banking details, social security number). Messages often include links or attachments. Phishing emails impersonate established companies, non-profits, charities, and government agencies.
	"Spear phishing" refers to spam targeted towards specific individuals.
Malware	Malicious apps/viruses hidden in email connections or apps designed to obtain sensitive personal information or damage computer systems.
Fraudulent eCommerce	Websites that sell counterfeit products, ship no products, or illegally sell regulated products.
Romance scams	Cybercriminal fakes an identity online to gain trust and then steals from or manipulates the victim.
Tech support scams	Cybercriminal sends email or pop-up message warning you have a computer problem, or a virus, often pretending to be from a well-known company, asks for remote access, to sell worthless tech support services, and/or installs malware to collect sensitive information.
Extortion/blackmail	Cybercriminal accuses the victim of inappropriate behavior, threatening to tell family, employers, social network contacts without immediate ransom payment, generally within 48 h in Bitcoin.
Work from home scams	Wide variety of scams targeting every aspect of work from home environments (communications, video conferencing, remote data sharing, etc.) to obtain sensitive personal information or extort.
Denial of service	Disruptive attacks, often large scale that make the websites of an organization or government service unavailable.

registered, with over 2000 malicious registrations, and over 40,000 high-risk registrations with evidence of association with malicious URLs [67]. Examples of medical cybercrime related to COVID-19 are shown in Table 2.

Vulnerability to Cybercrime

With the rapid and massive shift online, there is concern that individuals are insufficiently trained, are using unfamiliar

Table 2 Examples of online medical fraud related to COVID-19 aimed at individuals in the USA

Type of cybercrime	Example	Reference
Malware	Malware embedded in a fake global COVID-19 cases map, pretending to be a live map from Johns Hopkins University.	Reason Labs [68]
Phishing	Fraudulent email and WhatsApp messages pretending to be WHO with COVID-19 updates.	WHO [69]
Phishing	Website offering fake vaccine for COVID-19.	DOJ [70]
Phishing	Fraudulent messages on WhatsApp or Facebook offering coupons for food support.	FTC [71]
Phishing	Text messages impersonating USA HHS to take a "mandatory online COVID-19 test"	BBB [72]
Ransomware	Ransomware in a fake COVID-19 contact tracking phone app demanding bitcoin payment or lock out of phone and leak personal information.	Villas-Boas [73]
Extortion/Blackmail	Threatens the release of "dirty secrets" and to infect you and family with COVID-19 without immediate payment.	FBI [74]
Fraudulent eCommerce	Websites advertising items in short supply like masks. No product shipped.	BBB [75]
Fraudulent eCommerce	Websites posing as pharmacy with COVID-19 "treatments" to obtain personal information. No drugs shipped	Bolster [76]
Fraudulent eCommerce	Expansion of rogue, unlicensed, online pharmacies selling prescription drugs without a prescription, often substandard and dangerous, now advertising unproven "cures" for COVID-19.	NABP [77]
Zoombombing	Hijacking of conferences with pornography, hate images, and threats. Examples include Alcoholics Anonymous meetings and biomedical classes.	Lorenz [78], Walsh [79]

tools, are inexperienced with the technology, and, as a result, becoming easy targets for cybercriminals. In the UK, the increase in cybercrime during the pandemic mainly impacted individuals rather than organizations [80]. With cybercrime, individuals often actively participate in the fraudulent process to which they become the victim, such as by responding to a phishing email and providing private information [81]. Individuals may not be sufficiently suspicious, may not be able to detect fraudulent messages, or may not pay sufficient attention to stop a fraudulent process [81]. Falling for a scam involves errors in decision-making, and the spammers' goal is to create situations that increase the likelihood of errors in judgment [82]. Spammers make their offers look like they come from official institutions or legitimate businesses that people routinely trust [82], and use persuasion principles found to be effective in legitimate emails [83, 84].

Vulnerability to online fraud involves a combination of psychological and demographic factors, and online activities, where victim profiles vary with the type of cybercrime [85]. Overall, victims of online fraud are older, impulsive, sensation seeking, have an addictive disposition, and follow routine activities placing them at risk for fraud like online banking and shopping [10]. Victims of tech support scams are usually over age 50, and may have less technical familiarity than younger people [86]. Although older people have the highest risk of large financial loss, in 2020, many cybercrimes increased by at least 10% in all age groups, including phishing by text, online shopping scams, and romance scams [86]. Individuals with healthcare concerns may have increased susceptibility to health related phishing [87].

The malicious attempts by cybercriminals to influence people's behavior co-exist with the legitimate Internet business model based on "surveillance capitalism" [88]. Data from everyone's online activities and smart devices are collected, combined, and analyzed and packaged as products to predict and modify our behavior [88]. Additionally, many online products are designed to be addictive, to generate an instant response to a message, and maximize time spent with the product [89]. In other words, legal online manipulation defined as "the use of information technology to covertly influence another person's decision making, by targeting and exploiting their decision making vulnerabilities" is part of our lives [90]. Spammers' output may blend in with the background of individual messages tailored to people's habits. The routine behavioral manipulation from targeted online advertising may make it harder to discern fraudulent manipulation by cybercriminals.

The importance of human factors in cybercrime cannot be overstated. The problems of cybersecurity cannot be solved just by adding more technology. Humans are involved in every aspect of cybersecurity in our complex, interconnected, digitalized world as software and hardware developers, systems administrators, managers, end users, consumers, attackers, and victims. The ways in which humans interact with each other, process information and make decisions, handle workload and stress, and interface with technology are fundamental to cybersecurity. Humans often place inappropriate levels of trust in automated systems [91]. Research in cybersecurity is shifting from a primary focus on technology to recognize the central importance of human behavior, social, and cultural factors [2, 83]. Since the focus of most attacks is on human vulnerabilities, it is critical to understand how humans routinely interface with technology, including cybersecurity products. For example, consider the "prevalence effect," defined that when signals become less common they are substantially more difficult for an operator to detect [3•]. As modern anti-spam technology reduces the number of spam emails received, a user may be increasingly less likely to detect and report a cyberattack sent by email [3•].

Aftermath of Online Fraud

Victims of online fraud may face psychological effects as well as financial consequences [92]. Large, sudden economic losses are associated with mental health changes, especially depression, as found in Europe and the USA after the Great Recession of 2008 [93–95]. Victims of online fraud report that psychological effects of being scammed are felt as strongly as the financial impacts [92]. Victims of online romance scams also experience the loss of a relationship, and report feelings of depression, guilt, deep shame and embarrassment [96]. Victims of identity theft report considerable emotional distress including feeling anger, stress, and depression, as well as many physical symptoms [97, 98]. Online fraud may worsen the symptoms of mental illness, as stressful life events may trigger relapses in those with an enduring mental illness [42].

Mental Illness May Increase Vulnerability

Mental illness may increase vulnerability to cybercrime. People who are psychologically vulnerable, including those with severe mental illness, and older adults, may become victims of many types of financial fraud [99, 100]. People who are impulsive or emotionally unstable are more likely to lose money to online fraud [85]. Social isolation and the change to daily routines may disrupt the coping strategies and decrease social connections of those with mental illness [55]. Some people with mental illness may go online while experiencing psychotic symptoms, during a crises, or have some degree of cognitive or memory impairment. Lower short-term memory and negative affect in old age may contribute to increased risk of online deception [101]. Some adolescents have negative emotional effects from heavy use of social media or digital devices [102]. The digital divide remains, and some people go online irregularly, lack technical training and skills, which may increase vulnerability to fraud [103]. Additionally, when

individuals with less education become victims of online fraud, they often remain passive and do not evaluate their own actions to prevent future incidents [104].

Recommendations

Psychiatrists need to recognize the increasing risks of cybercrime, and that patients may be unaware of these risks. Many people have no formal training in technology, and have limited skills and knowledge. Patients may not recognize the need for cybersecurity, understand which online behaviors are risky, know how to implement cybersecurity measures, or how to report a cybercrime. When patients are prescribed medications, they are given instructions by the prescriber, and receive printed information from the pharmacy that includes instructions, cautions, and possible side effects. Similarly, patients should be made aware that there are serious risks of cybercrime when going online for all purposes, including mental health related services. We suggest that psychiatrists who use or recommend technology provide patients with a list of trusted sources that educate consumers on how to recognize and lessen the risk of cybercrime. Examples of USA governmental agencies that provide cybersecurity information for consumers are shown in Table 3. With the large increase in disinformation and the registration of phony domains since the pandemic, providing trusted sources of cybersecurity advice becomes more important.

Providing information sources will not prevent patients from experiencing online fraud, and the role of the psychiatrist is not to teach about cybercrime and cybersecurity. We do suggest that distributing information will increase the awareness of cybersecurity and encourage individuals to educate themselves using information from professional organizations that deal with cybercrime. Likewise, if telemedicine is used for psychiatric visits, trusted technical sources should be provided for training and ongoing support on the specific telemedicine product.

The problem of cybercrime prevention has no easy solution. Home computers and home networks are often out of date, without the latest security patches, and lacking antivirus protection. Younger people may be less aware of cybersecurity and less likely to follow recommended policies [105, 106]. Even technically sophisticated people fall victim to phishing due to a lack of cognitive involvement when processing emails [107]. Given the increased vulnerability to cybercrime for those with mental illness, and the long-term negative psychological and financial impacts for victims, it is important to increase awareness of cybercrime. Many patients may not know where to go for help with cybersecurity issues. Providing trusted information is an important first step.

Limitations

Many individuals are victims of a corporate data breach, but cybercrime against corporations or universities was not included. In an international study, healthcare was the industry with the highest average data breach costs [108]. Attacks against research organizations related to COVID-19 were not included [109]. Employer-related cybersecurity issues for those working at home were not included. The measures

Table 3 Examples of USA organizations that provide advice about cybersecurity for consumers

Organization	Source	Website
FBI	The Cyber Threat. What You Should Know Sections include "Protect yourself" and "Understand Common Crimes and Risks Online"	https://www.fbi.gov/investigate/cyber
Oregon FBI	Tech Tuesday. Article every Tuesday about cybersecurity for consumers. Example: Cyber Security Awareness Month	https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-cyber-security-awareness-month
CISA (Cybersecurity and Infrastructure Security Agency)	Tips. "Tips describe and offer advice about common security issues for non-technical computer users"	https://us-cert.cisa.gov/ncas/tips
FTC (Federal Trade Commission)	Coronavirus Advice for Consumers. Avoid Coronavirus Scams.	https://www.ftc.gov/coronavirus/scams-consumer-advice
FDA	Medical Device Cybersecurity: What You Need to Know	https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

available to prevent cybercrime for individuals or employees, the effectiveness of these measures, and training approaches to teach about cybersecurity were not discussed. International legal structures, challenges in investigating and prosecuting cybercrime, and policing resources spent on cybercrime were not discussed. The presence of mental illness in those who commit cybercrime was not discussed.

Conclusion

Since the pandemic, there has been a dramatic shift online for routine activities including work, school, shopping, entertainment and doctor visits, and a surge in cybercrime. Technology provides powerful tools but these tools must be used with the appropriate safety measures. Human factors are a central component of cybersecurity as individual behaviors, personality traits, online activities, and attitudes to technology impact susceptibility. Mental illness may increase vulnerability to cybercrime, yet patients may not be aware of the dangers, risky online behaviors, or measures to mitigate risk. Psychiatrists should be aware of the potential aftermath of cybercrime on mental health, and the increased patient risk since the pandemic, including from online mental health services. With the long-term psychological and financial consequences experienced by victims of cybercrime, it is important to increase patient awareness of cybersecurity. As a first step, psychiatrists should provide a recommended list of trusted sources that educate consumers on cybersecurity.

Compliance with Ethical Standards

Human and Animal Rights and Informed Consent This article does not contain any studies with human or animal subjects performed by any of the authors.

References

Papers of particular interest, published recently, have been highlighted as:
- Of importance

1. Gutzwiller RS, Fugate S, Sawyer BD, Hancock PA. The human factors of cyber network defense. In: In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 59. 1st ed. Sage: SAGE publications; 2015. p. 322–6.
2. Proctor RW, Chen J. The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. Hum Factors. 2015;57:721–7.
3. • Sawyer BD, Hancock PA. Hacking the human: the prevalence paradox in cybersecurity. Hum Factors. 2018;60:597–609 **Study of prevalence effects in email cybersecurity and discussion of human-computer interface.**
4. CISA. (Cybersecurity and Infrastructure Security Agency), "Alert (AA20-099A): COVID-19 exploited by malicious cyber actors," April 8, 2020. https://www.us-cert.gov/ncas/alerts/aa20-099a Accessed 3 Dec 2020.
5. Interpol. Cybercrime: Covid-19 impact. Aug 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 Accessed 3 Dec 2020.
6. Shivers CA. COVID-19 fraud: law enforcement's response to those exploiting the pandemic. Statement before the Senate Judiciary Committee. June 9, 2020. https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic Accessed 3 Dec 2020.
7. WEF (World Economic Forum). The global risks report 2019. https://www.weforum.org/reports/the-global-risks-report-2019 Accessed 3 Dec 2020.
8. McAfee. The economic impact of cybercrime—no slowing down. 2018. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html Accessed 3 Dec 2020.
9. Jeong J, Mihelcic J, Oliver G, Rudolph C. Towards an improved understanding of human factors in cybersecurity. In2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) 2019 Dec 12 (pp. 338-345). IEEE.
10. Whitty MT. Predicting susceptibility to cyber-fraud victimhood. J Financial Crime. 2019;26:277–92.
11. Monteith S, Glenn T. Automated decision-making and big data: concerns for people with mental illness. Curr Psychiatry Rep. 2016;18:112.
12. OECD. (Organisation for Economic Co-operation and Development). Keeping the Internet up and running in times of crisis. May 4, 2020. https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/ Accessed 3 Dec 2020.
13. NCTA. (The Internet & Television Association). COVID-19: How cable's Internet networks are performing. Metrics, trends & observations. 2020. https://www.ncta.com/COVIDdashboard Accessed 3 Dec 2020.
14. Gartner. Gartner says global smartphone sales declined 20% in first quarter of 2020 due to COVID-19 impact. June 1, 2020. https://www.gartner.com/en/newsroom/press-releases/2020-06-01-gartner-says-global-smartphone-sales-declined-20–in- Accessed 3 Dec 2020.
15. Gartner. Gartner says global smartphone sales declined 20% in second quarter of 2020. August 25, 2020 https://wwwgartnercom/en/newsroom/press-releases/2020-08-25-gartner-says-global-smartphone-sales-declined-20–in- Accessed 3 Dec 2020.
16. GSMA. IoT connections forecast: the impact of Covid-19. June 8, 2020. https://www.gsma.com/iot/resources/iot-connections-forecast-the-impact-of-covid-19/ Accessed 3 Dec 2020.
17. IDC. Traditional PC shipments continue to grow amid global economic slowdown, according to IDC. July 9, 2020. https://www.idc.com/getdoc.jsp?containerId=prUS46691020 Accessed 3 Dec 2020.
18. OSU (Ohio State University). Survey finds American's social media habits changing as national tensions rise. Aug 3, 2020. https://wexnermedical.osu.edu/mediaroom/pressreleaselisting/survey-finds-americans-social-media-habits-changing-as-national-tensions-rise Accessed 3 Dec 2020.
19. Cohen J. Data usage has increased 47 percent during COVID-19 quarantine. PCMag. June 5, 2020. https://www.pcmag.com/news/data-usage-has-increased-47-percent-during-covid-19-quarantine Accessed 3 Dec 2020.
20. CRR (Centre for Retail Research). Online: UK, Europe & N. America 2020 estimates. 2020. https://www.retailresearch.org/online-retail.html Accessed 3 Dec 2020.

21. Garratt R, Lee M, Plesset A. COVID-19 and the search for digital alternatives to cash," Federal Reserve Bank of New York *Liberty Street Economics*, September 28, 2020. https://libertystreeteconomics.newyorkfed.org/2020/09/covid-19-and-the-search-for-digital-alternatives-to-cash.html Accessed 3 Dec 2020.
22. Toh YL, Tran T. How the COVID-19 pandemic may reshape the digital payments landscape. Federal Reserve Bank of Kansas City Main Street Views. June 24, 2020. https://www.kansascityfed.org/en/publications/research/rwp/psrb/articles/2020/covid19-pandemic-may-reshape-digital-payments-landscape Accessed 3 Dec 2020.
23. Öngür D, Perlis R, Goff D. Psychiatry and COVID-19. JAMA. 2020;324:1149–50.
24. Mansour O, Tajanlangit M, Heyward J, Mojtabai R, Alexander GC. Telemedicine and office-based care for behavioral and psychiatric conditions during the COVID-19 pandemic in the United States. Ann Intern Med. 2020. https://doi.org/10.7326/M20-6243.
25. Chen JA, Chung WJ, Young SK, Tuttle MC, Collins MB, Darghouth SL, et al. COVID-19 and telepsychiatry: early outpatient experiences and implications for the future. Gen Hosp Psychiatry. 2020;66:89–95.
26. Connolly SL, Stolzmann KL, Heyworth L, Weaver KR, Bauer MS, Miller CJ. Rapid increase in telemental health within the Department of Veterans Affairs during the COVID-19 pandemic. Telemed J E Health. 2020. https://doi.org/10.1089/tmj.2020.0233.
27. Rosic T, Lubert S, Samaan Z. Virtual psychiatric care fast-tracked: reflections inspired by the COVID-19 pandemic. BJPsych Bull. 2020;17:1–4.
28. Shore JH, Schneck CD, Mishkind MC. Telepsychiatry and the coronavirus disease 2019 pandemic-current and future outcomes of the rapid virtualization of psychiatric care. JAMA Psychiatry. 2020. https://doi.org/10.1001/jamapsychiatry.2020.1643
29. World Bank. COVID-19 to add as many as 150 million extreme poor by 2021, 2020. Press release no: 2021/024/DEC-GPV https://www.worldbank.org/en/news/press-release/2020/10/07/covid-19-to-add-as-many-as-150-million-extreme-poor-by-2021 Accessed 3 Dec 2020.
30. RWJ Foundation, NPR, Harvard TH. Chan School of Public Health. The impact of coronavirus on households in major U.S. cities. 2020. https://www.rwjf.org/en/library/research/2020/09/the-impact-of-coronavirus-on-households-across-america.html Accessed 3 Dec 2020.
31. Hermann A, Cornelissen S. Using the Census Bureau's Household Pulse Survey to assess the economic impacts of COVID-19 on America's households. Harvard Joint Center for Housing Studies Housing Perspectives. 2020. https://www.jchs.harvard.edu/blog/using-the-census-bureaus-household-pulse-survey-to-assess-the-economic-impacts-of-covid-19-on-americas-households/ Accessed 3 Dec 2020.
32. Armantier O, Koşar G, Pomerantz R, van der Klaauw W. The disproportionate effects of COVID-19 on households with children. Federal Reserve Bank of New York *Liberty Street Economics*. 2020. https://libertystreeteconomics.newyorkfed.org/2020/08/the-disproportionate-effects-of-covid-19-on-households-with-children.html Accessed 3 Dec 2020.
33. Monte LM. US Census Bureau. New Census Household Pulse Survey shows more households with children lost income, experienced food shortages during pandemic. 2020. https://www.census.gov/library/stories/2020/05/adults-in-households-with-children-more-likely-to-report-loss-in-employment-income-during-covid-19.html Accessed 3 Dec 2020. Accessed 3 Dec 2020.
34. Fry R, Passel JS, Cohn D. A majority of young adults in the U.S. live with their parents for the first time since the Great Depression. Pew Research. 2020. https://www.pewresearch.org/fact-tank/2020/09/04/a-majority-of-young-adults-in-the-u-s-live-with-their-parents-for-the-first-time-since-the-great-depression/ Accessed 3 Dec 2020.
35. Brooks SK, Webster RK, Smith LE, Woodland L, Wessely S, Greenberg N, et al. The psychological impact of quarantine and how to reduce it: rapid review of the evidence. Lancet. 2020;395:912–20.
36. Bu F, Steptoe A, Fancourt D. Who is lonely in lockdown? Cross-cohort analyses of predictors of loneliness before and during the COVID-19 pandemic. Public Health. 2020;186:31–4.
37. Twenge JM, Joiner TE. U.S. Census Bureau-assessed prevalence of anxiety and depressive symptoms in 2019 and during the 2020 COVID-19 pandemic. Depress Anxiety. 2020. https://doi.org/10.1002/da.23077.
38. Winkler P, Formanek T, Mlada K, Kagstrom A, Mohrova Z, Mohr P, et al. Increase in prevalence of current mental disorders in the context of COVID-19: analysis of repeated nationwide cross-sectional surveys. Epidemiol Psychiatr Sci. 2020;29:e173.
39. Xiong J, Lipsitz O, Nasri F, Lui LMW, Gill H, Phan L, et al. Impact of COVID-19 pandemic on mental health in the general population: a systematic review. J Affect Disord. 2020;277:55–64.
40. Elbogen EB, Lanier M, Montgomery AE, Strickland S, Wagner HR, Tsai J. Financial strain and risk of suicide in the wake of the COVID-19 pandemic. Am J Epidemiol. 2020;22:kwaa149. https://doi.org/10.1093/aje/kwaa149.
41. Ettman CK, Gradus JL, Galea S. Reckoning with the relation between stressors and suicide attempts in a time of Covid-19. Am J Epidemiol. 2020;22:kwaa147. https://doi.org/10.1093/aje/kwaa147.
42. Lazzari C, Shoka A, Nusair A, Rabottini M. Psychiatry in time of COVID-19 pandemic. Psychiatr Danub. 2020 Summer;32:229–35.
43. Fegert JM, Vitiello B, Plener PL, Clemens V. Challenges and burden of the coronavirus 2019 (COVID-19) pandemic for child and adolescent mental health: a narrative review to highlight clinical and research needs in the acute phase and the long return to normality. Child Adolesc Psychiatry Ment Health. 2020;14:20.
44. Liu CH, Stevens C, Conrad RC, Hahm HC. Evidence for elevated psychiatric distress, poor sleep, and quality of life concerns during the COVID-19 pandemic among U.S. young adults with suspected and reported psychiatric diagnoses. Psychiatry Res. 2020;292:113345. https://doi.org/10.1016/j.psychres.2020.113345.
45. Bäuerle A, Steinbach J, Schweda A, Beckord J, Hetkamp M, Weismüller B, et al. Mental health burden of the COVID-19 outbreak in Germany: predictors of mental health impairment. J Prim Care Community Health. 2020;11:2150132720953682. https://doi.org/10.1177/2150132720953682.
46. Hao F, Tan W, Jiang L, Zhang L, Zhao X, Zou Y, et al. Do psychiatric patients experience more psychiatric symptoms during COVID-19 pandemic and lockdown? A case-control study with service and research implications for immunopsychiatry. Brain Behav Immun. 2020;87:100–6.
47. McCracken LM, Badinlou F, Buhrman M, Brocki KC. Psychological impact of COVID-19 in the Swedish population: depression, anxiety, and insomnia and their associations to risk and vulnerability factors. Eur Psychiatry. 2020;63:e81.
48. Asmundson GJG, Paluszek MM, Landry CA, Rachor GS, McKay D, Taylor S. Do pre-existing anxiety-related and mood disorders differentially impact COVID-19 stress responses and coping? J Anxiety Disord. 2020;74:102271.
49. Da BL, Im GY, Schiano TD. COVID-19 hangover: a rising tide of alcohol use disorder and alcohol-associated liver disease. Hepatology. 2020;72:1102–8.

50. McKay D, Asmundson GJG. COVID-19 stress and substance use: current issues and future preparations. J Anxiety Disord. 2020;74: 102274.
51. ACHP (Alliance of Community Health Plans). Breakdown of changes in consumers' health care behavior during COVID-19. 5/21/20. https://achp.org/research-breakdown-of-changes-in-consumers-health-care-behavior-during-covid-19/ Accessed 3 Dec 2020.
52. Hamel L, Kearney A, Kirzinger A, Lopes L, Munana C, Brodie M. KFF Health Tracking Poll-May 2020. Kaiser Family Foundation. 2020. https://www.kff.org/coronavirus-covid-19/report/kff-health-tracking-poll-may-2020/ Accessed 3 Dec 2020.
53. Kahl KG, Correll CU. Management of patients with severe mental illness during the coronavirus disease 2019 pandemic. JAMA Psychiatry. 2020;77:977–8.
54. Shinn AK, Viron M. Perspectives on the COVID-19 pandemic and individuals with serious mental illness. J Clin Psychiatry. 2020;81:20com13412.
55. Costa M, Pavlo A, Reis G, Ponte K, Davidson L. COVID-19 concerns among persons with mental illness. Psychiatr Serv. 2020;3:appips202000245. https://doi.org/10.1176/appi.ps.202000245.
56. Goldenberg MN, Parwani V. Psychiatric emergency department volume during Covid-19 pandemic. Am J Emerg Med. 2020;1: S0735–6757(20)30450–2.
57. Gonçalves-Pinho M, Mota P, Ribeiro J, Macedo S, Freitas A. The impact of COVID-19 pandemic on psychiatric emergency department visits-a descriptive study. Psychiatr Q. 2020;25:1–11. https://doi.org/10.1007/s11126-020-09837-z.
58. Hoyer C, Ebert A, Szabo K, Platten M, Meyer-Lindenberg A, Kranaster L. Decreased utilization of mental health emergency service during the COVID-19 pandemic. Eur Arch Psychiatry Clin Neurosci. 2020;9:1–3. https://doi.org/10.1007/s00406-020-01151-w.
59. Huang K, Siegel M, Madnick S. Systematically understanding the cyber attack business: a survey. ACM Comp Surv (CSUR). 2018;51:1–36.
60. Ablon L, Libicki MC, Golay AA. Markets for cybercrime tools and stolen data: hackers' bazaar. Rand Corporation; 2014.
61. Conteh NY, Royer MD. The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. Int J Comp (IJC). 2016;20:1–2.
62. Brown S. How to think about cybersecurity in the era of COVID-19. Ideas Made to Matter. MIT Sloan. 2020. https://mitsloan.mit.edu/ideas-made-to-matter/how-to-think-about-cybersecurity-era-covid-19 Accessed 3 Dec 2020.
63. Patel A, Hatzakis T., Macnish K, Ryan M, Kirichenko A. Security issues, dangers and implications of smart information systems. Project Sherpa. 2019. https://blog-assets.f-secure.com/wp-content/uploads/2019/07/23170423/d1.3-cyberthreats-and-countermeasures.pdf Accessed 3 Dec 2020.
64. Iriondo R. Breaking CAPTCHA using machine learning in 0.05 seconds. Medium.com. 2020. https://medium.com/towards-artificial-intelligence/breaking-captcha-using-machine-learning-in-0-05-seconds-9feefb997694 Accessed 3 Dec 2020.
65.• FBI. The cyber threat. 2020. https://www.fbi.gov/investigate/cyber Accessed 3 Dec 2020. **Current information on cybersecurity for the general public.**
66. UN. UN News, 2020. Illegal trade in fake or faulty COVID-19 products booming, new UN research reveals. https://news.un.org/en/story/2020/07/1067831 Accessed 3 Dec 2020.
67. Szurdi J, Chen Z, Starov O, McCabe A, Duan R. Palo Alto Networks, 2020. Studying how cybercriminals prey on the COVID-19 pandemic. https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/ Accessed 3 Dec 2020.
68. Reason Labs. COVID-19, Info stealer & the map of threats–threat analysis report. 2020. https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/ Accessed 3 Dec 2020.
69. WHO. Beware of criminals pretending to be WHO. 2020. https://www.who.int/about/communications/cyber-security Accessed 3 Dec 2020.
70. DOJ (US Department of Justice). Justice Department files its first enforcement action against COVID-19 fraud. 2020. https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud Accessed 3 Dec 2020.
71. FTC (US Federal Trade Commission). Those free COVID-19 money offers on WhatsApp and Facebook are scams. Aug. 28, 2020. https://www.consumer.ftc.gov/blog/2020/08/those-free-covid-19-money-offers-whatsapp-and-facebook-are-scams Accessed 3 Dec 2020.
72. BBB (Better Business Bureau). BBB scam alert: "mandatory" COVID-19 test texts are a scam. Oct 6, 2020. https://www.bbb.org/article/news-releases/21903-scam-alert-mandatory-covid-19-test-texts-are-a-scam Accessed 3 Dec 2020.
73. Villas-Boas A. A fake coronavirus tracking app is actually ransomware that threatens to leak social media accounts and delete a phone's storage unless a victim pays $100 in bitcoin. Business Insider. 2020. https://www.businessinsider.com/coronavirus-fake-app-ransomware-malware-bitcoin-android-demands-ransom-domaintools-2020-3 Accessed 3 Dec 2020.
74. FBI. FBI Expects a rise in scams involving cryptocurrency related to the COVID-19 pandemic. 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic Accessed 3 Dec 2020.
75. BBB (Better Business Bureau). BBB scam alert: preparing for mask mandates? Watch out for online cons. 2020 https://www.bbb.org/article/news-releases/21482-scam-alert-preparing-for-coronavirus-that-face-mask-could-be-a-con Accessed 3 Dec 2020.
76. Bolster Q FY 2020 State of phishing & online fraud. 2020. https://bolster.ai/reports Accessed 3 Dec 2020.
77. NABP (US National Association of Boards of Pharmacy). Rogue online pharmacies in the time of pandemic:capitalizing on misinformation and fear. 2020. https://nabp.pharmacy/wp-content/uploads/2020/05/Rogue-Rx-Activity-Report-May-2020.pdf Accessed 3 Dec 2020.
78. Lorenz T, Alba D. 'Zoombombing' becomes a dangerous organized effort. The New York Times. 2020. https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html Accessed 3 Dec 2020.
79. Walsh CG, Unertl KM, Ebert JS. Rapid supportive response to a traumatic "zoombombing" during the COVID-19 pandemic. Acad Med. 2020;96:e6–7. https://doi.org/10.1097/ACM.0000000000003739.
80. Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S, Díaz-Castaño N. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. Eur Soc. 2020;12:1–3.
81. Jansen J, Leukfeldt R. How people help fraudsters steal their money: an analysis of 600 online banking fraud cases. In: 2015 workshop on socio-technical aspects in security and trust 2015 (pp. 24-31). IEEE.
82. Lea SE, Fischer P, Evans KM. The psychology of scams: Provoking and committing errors of judgement. A report for the UK Office of Fair Trading. 2009. https://ore.exeter.ac.uk/repository/handle/10871/20958 Accessed 3 Dec 2020.
83. Corradini I. Redefining the approach to cybersecurity. In: In: Building a cybersecurity culture in organizations. Cham: Springer; 2020. p. 49–62.
84. Lawson P, Pearson CJ, Crowson A, Mayhorn CB. Email phishing and signal detection: how persuasion principles and personality

influence response patterns and accuracy. Appl Ergon. 2020;86: 103084.
85. Whitty MT. Is there a scam for everyone? Psychologically profiling cyberscam victims. Eur J Crim Policy Res. 2020;26:399–409.
86. Payne BK. Criminals work from home during pandemics too: a public health approach to respond to fraud and crimes against those 50 and above. Am J Crim Justice. 2020;11:1.
87. Abdelhamid M. The role of health concerns in phishing susceptibility: survey design study. J Med Internet Res. 2020;22:e18394.
88. Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: PublicAffairs; 2019.
89. Alter A. Irresistible: the rise of addictive technology and the business of keeping us hooked. New York: Penguin Press; 2017.
90. Susser D, Roessler B, Nissenbaum H. Technology, autonomy, and manipulation. Internet Policy Rev. 201930;8(2). DOI: https://doi.org/10.14763/2019.2.1410.
91. Lee JD, See KA. Trust in automation: designing for appropriate reliance. Hum Factors. 2004;46:50–80.
92. Modic D, Anderson R. It's all over but the crying: the emotional and financial impact of Internet fraud. IEEE Secur Priv. 2015;13: 99–103.
93. Forbes MK, Krueger RF. The great recession and mental health in the United States. Clin Psychol Sci. 2019;7:900–13.
94. Marazziti D, Avella MT, Mucci N, Della Vecchia A, Ivaldi T, Palermo S, et al. Impact of economic crisis on mental health: a 10-year challenge. CNS Spectr 2020:1–7.
95. McInerney M, Mellor JM, Nicholas LH. Recession depression: mental health effects of the 2008 stock market crash. J Health Econ. 2013;32:1090–104.
96. Whitty MT, Buchanan T. The online dating romance scam: the psychological impact on victims–both financial and non-financial. Criminol Crim Just. 2016;16:176–94.
97. ITRC (Identity Theft Resource Center). Identity theft. The Aftermath Study 2017. 2017. https://www.idtheftcenter.org/identity-theft-aftermath-study/ Accessed 3 Dec 2020.
98. Golladay K, Holtfreter K. The consequences of identity theft victimization: an examination of emotional and physical health outcomes. Vict Offenders. 2017;12:741–60.
99. Claycomb M, Black AC, Wilber C, Brocke S, Lazar CM, Rosen MI. Financial victimization of adults with severe mental illness. Psychiatr Serv. 2013;64:918–20.
100. Lichtenberg PA, Sugarman MA, Paulson D, Ficker LJ, Rahman-Filipiak A. Psychological and functional vulnerability predicts fraud cases in older adults: results of a longitudinal study. Clin Gerontol. 2016;39:48–63.
101. Ebner NC, Ellis DM, Lin T, Rocha HA, Yang H, Dommaraju S, et al. Uncovering susceptibility risk to online deception in aging. J Gerontol B Psychol Sci Soc Sci. 2020;75:522–33.
102. Abi-Jaoude E, Naylor KT, Pignatiello A. Smartphones, social media use and youth mental health. CMAJ. 2020;192:E136–41.
103. Gangadharan SP. The downside of digital inclusion: expectations and experiences of privacy and surveillance among marginal Internet users. New Media Soc. 2017;19:597–615.
104. Scheerder AJ, van Deursen AJ, van Dijk JA. Negative outcomes of Internet use: a qualitative analysis in the homes of families with different educational backgrounds. Inf Soc. 2019;35:286–98.
105. Hadlington L, Chivers S. Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors. Policing: A Journal of Policy and Practice. 2020;14:479–92.
106. Debb SM, Schaffer DR, Colson DG. A reverse digital divide: comparing information security behaviors of generation Y and generation Z adults. Int J Cybersecurity Intell Cybercrime. 2020;3:42–55.
107. Vishwanath A, Herath T, Chen R, Wang J, Rao HR. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decis Support Syst. 2011;51:576–86.
108. IBM and Ponemon Institude. Cost of a data breach report 2020. https://www.ibm.com/security/data-breach Accessed 3 Dec 2020.
109. FBI. People's Republic of China (PRC) Targeting of COVID-19 Research Organizations. 2020. May 13, 2020. https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations Accessed 3 Dec 2020.