JYX JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Woods, Naomi

Title: Users' Psychopathologies : Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior

Year: 2022

Version: Accepted version (Final draft)

Copyright: © 2022 The Author(s), under exclusive license to Springer Nature Switzerland AG

Rights: In Copyright

Rights url: http://rightsstatements.org/page/InC/1.0/?language=en

Please cite the original version:

Woods, N. (2022). Users' Psychopathologies : Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior. In M. Lehto, & P. Neittaanmäki (Eds.), Cyber Security : Critical Infrastructure Protection (pp. 93-134). Springer. Computational Methods in Applied Sciences, 56. https://doi.org/10.1007/978-3-030-91293-2_5

Users' Psychopathologies Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior

Naomi Woods
Faculty of Information Technology, University of Jyväskylä, Finland
naomi.woods@jyu.fi

Abstract: The internet and digital technologies have become an integral part of people's daily lives. The online world provides many benefits to billions of users globally. However, it also brings risks too, because it is easy for criminals to reach their victims and exploit their online behavior. Nevertheless, users often perform risky security behaviors for convenience and usability, and because of their inadequate security awareness. With around 25% of the world's population experiencing mental and/or neurological disorders, it is important to understand how users' psychopathologies manifest themselves in the context of cybersecurity. This chapter has reviewed the symptoms of several mental disorders while considering the online benefits and risks, and these symptoms have been applied to evaluate users' vulnerability to cybercrimes and cybersecurity practices. The findings reveal how the complexity of each mental disorder influences users' online engagement and susceptibility to cybercrimes, and how uniquely, to varying degrees, they affect different cybersecurity behaviors.

Keyword Cybersecurity behavior, Psychopathology, Mental disorder, Cybercrime, Online benefits, Online risks, User psychology, Cyberpsychology

5.1 Introduction

Over the last few decades, digitalization has changed our society. Today, technology is integral to nearly every part of our lives [1]. At home, from the moment we wake, the lights we put on, and the electricity we use to make coffee—it all comes from or is managed by systems that are digitalized. Most of us use our phones and smart devices throughout our day. Digital systems can also be found in nearly all working environments—we do not even have to work in an office to use a computer. From farming to manufacturing and many other industries interacting with machinery, all have digitalized systems [2]. We also communicate mainly online and have so many platforms and services available. We bank, we shop, our entertainment, all online. And as technology develops, more and more services and devices will become smart, including many infrastructures. Furthermore, our personal identity is online too. Therefore, with so many digital services, systems, and personal and organizational information online, cybersecurity and securing these assets can be considered just as important as the assets themselves [3, 4].

There are regular reports in the news or on social media referring to some sort of cyberattack [5]. Even though cybersecurity has developed immensely and is constantly evolving, cybercrime is growing, and criminals are always one step ahead. Many complex protocols have been developed by cybersecurity professionals and, when employed properly, provide a strong defense [6]. If a user, even with the strongest protocols, creates a password from their pet's name or modifies the pass- word for other accounts using predictable patterns, such insecure security behavior will ultimately undermine all security efforts [7, 8].

To attempt to improve users' security practices, users (within organizations and at home) are provided with digital security guidance, made aware of threats, and have technological restrictions imposed [9].

Nonetheless, many users will circumvent security policies and safety protocols for the sake of convenience and usability [10, 11]. This can have catastrophic repercussions with millions of euros and dollars are lost globally due to security breaches, not to mention the threat to public safety when information and records are stolen if breaches succeed [12].

There are several reasons that users are thought to adopt unsafe security practices, including a lack of awareness of security threats, a lack of awareness of the consequences of their actions, and also a lack of knowledge of how security actually works. Many users do not realize how severe a security breach could be or how it could impact their lives and the lives around them [13–15]. Many are not even aware of how vulnerable they are to a potential threat, or to the damage it can cause [16]. However, when one thinks about what creates that awareness, understanding of behavioral consequences, and knowledge, and how a user considers it, processes it, stores it, and acts on it, each user will have many individual factors that affect each part of the process. Through understanding the individual differences of users, allows cybersecurity professionals to understand why the user is the "weakest link in security" [8, 17, 18]. Therefore, it is increasingly acknowledged that cybersecurity professionals not only need to have backgrounds in computer science and engineering, they also need to have backgrounds in the human, behavioral and cognitive sciences to comprehend the user and their security behavior [6, 17].

Due to the immense usage of technology, the digital user can be potentially anyone nowadays, including children, the elderly, people with disabilities, and people with mental disorders. There are over 4.3 billion internet users [19]. However, in 2001 the World Health Organization [20] estimated that one in every four people (25%) has a mental or neurological disorder, at around 450 Million people globally. This number has gone up over the years, with growing populations [20]. This means

that about 25% of digital users (just under 1.1 Billion) are living with some form of mental disorder. Therefore, the way these users interact with digital technology and the online world, and especially the way they interact with cybersecurity needs to be taken into consideration.

Over the years, research towards studying the usage of technology has been conducted by computer scientists, mathematicians, and engineers. It has only been in more recent times that researchers with a human sciences background have started to examine how users and societies interact with digital technologies [21]. This has led to the emergence of cyberpsychology as an applied psychological discipline [22]. One area of research within this discipline consists of the examination of psychopathology and abnormal behaviors, and how interacting with the internet and digital technology can affect users' mental and psychological states. One example includes the emergence of the internet, social media, internet abuse and online gaming addictions [23–25]. However, there is still very little research examining how users' psychopathology affects their interaction online, and next to no research considering how users' psychopathology affects the way they interact with cybersecurity. To address this gap, this chapter will discuss common psychopathologies and online interaction. It will consider the characteristics of specific mental disorders, and what online benefits, risks, and security issues bring to these users. It will examine online benefits and risks specific to each disorder, including vulnerability to cyber- crimes, and consider the impact psychopathologies have on the users' interaction with cybersecurity in an attempt to secure their digital lives.

5.2 Psychopathology and Abnormal Psychology

There are many areas of psychology examining different aspects of human beings, including social, behavioral, cognitive, physiological, neuropsychological, etc. Clin- ical psychology is a research-based practice,

concerned with examining, diagnosing, and providing care for individuals exhibiting a broad spectrum of abnormal behaviors and psychopathologies [26, 27].

Abnormal psychology studies unusual or atypical behaviors, thoughts, and emotions that are symptomatic of mental, behavioral, or neurological disorders. One criterion is that they are severe enough to negatively impede upon an individual's life and negatively impact (or to the extent to) how the individual interacts with society [24, 27]. Clinical psychologists employ different approaches to under- stand and treat abnormal behaviors. There are four main schools: psychodynamic, humanistic, behavioral and cognitive-behavioral, as well as systemic/family. These approaches examine and treat the individual, often observing the behavior, consid- ering the biological bases, and the internal thought processes indicative of mental disorders [27, 28]. Many clinicians will combine different approaches to provide successful treatment of different disorders. However, before treatment of abnormal behaviors and psychopathologies can be determined, diagnosis is first needed [29].

5.2.1 Classifying Psychopathology

Diagnosis is essential to the practice of psychology and psychiatry. It can take many years for mental health practitioners and clinicians to learn and become experts in formulating a diagnosis. Diagnostic manuals provide guidance, descriptions of symptoms, and criteria for diagnosing mental disorders. These manuals provide practitioners with a standardized language and an understanding to increase the reliability of diagnoses while reducing susceptibility to practitioner bias [30]. The two main diagnostic manuals for categorizing abnormal behavior, are the International Statis- tical Classification of Diseases and Related Health Problems (ICD) [31], and the Diagnostic and Statistical Manual of Mental Disorders (DSM) [29]. The ICD is a broader standardized tool,

encompassing all medical conditions. The ICD includes a chapter dedicated to “Mental and behavioral disorders” [31]. Both manuals categorize symptoms of abnormal behavior into disorders through the individual meeting specific criteria. While the ICD is thought to be used more frequently in Europe, the DSM is more frequently used in the US. However, both are employed globally. For the purposes of this chapter, we will use the DSM to look at psychopathologies and their impact on the cybersecurity context.

The DSM was first published by the American Psychiatric Association (APA) in 1952 and has seen many revisions over the years as clinical psychology has evolved with the times. The most recent edition, the DSM-5 was published in 2013 and is globally used by mental health practitioners, and researchers. Developed from the scientific advances in brain imaging techniques, neuroscience, and genetics, the manual was reorganized around psycho-physiological relationships rather than just common symptoms. This has led to the classification of 19 main classes with over 100 specific disorders. The most recent version of the DSM has also been modified to be more “harmonized” with ICD-11 (the most recent version) [29]. Although both manuals, (DSM and ICD) have proven to be useful, through the years they have also been considered controversial due to cultural, political bias, societal norms that influenced what is classified as a disorder or not. Further controversy has always arisen regarding the labeling of individuals. Many people believe that once one has been given a diagnosis, one is stuck with that diagnosis or “label”. Being labeled as one thing or another often provides others a reason to act in a specific way based on the label rather than the individual [24, 28, 30]. However, the counterargument highlights the need for diagnosis, as, without it, the correct treatment cannot be provided [27].

5.2.2 Mental Disorder

DSM-5 includes an overall definition of a mental disorder as:

A mental disorder is a syndrome characterized by clinically significant disturbance in an individual's cognition, emotion regulation, or behavior that reflects a dysfunction in the psycho- logical, biological, or developmental processes underlying mental functioning. Mental disorders are usually associated with significant distress or disability in social, occupational, or other important activities. An expectable or culturally approved response to a common stressor or loss, such as the death of a loved one, is not a mental disorder. Socially deviant behavior (e.g., political, religious, or sexual) and conflicts that are primarily between the individual and society are not mental disorders unless the deviance or conflict results from a dysfunction in the individual, as described above. ([29], p. 20)

This definition does not include all the features of every specific mental disorder. However, each mental disorder is characterized and described under each class within the manual. Each disorder can be diverse with a wide range of characteristics. These diverse characteristics and the severity of these characteristics can affect the way in which the user interacts with the internet and digital technology.

5.3 Online Benefits, Risks, and Security Behavior

In the days before mass digitalization and the internet, individuals with mental disorders could find themselves isolated and lonely. As the only form of interaction with society was oftentimes face-to-face encounters, and societal participation proved difficult for many. Nowadays, although engaging with the online world brings many benefits and opportunities, it can also bring risks, which will differ for each disorder. Along with these risks, there are potential vulnerabilities to cybercrimes, and vulnerabilities in the users' cybersecurity behaviors they adopt to protect themselves.

5.3.1 Benefits of Online Interaction

Engaging with digital technologies and interacting online can provide

many benefits for users who have psychopathologies. The opportunities for being more integrated into society, contributing to society, and being supported by society have consider- ably grown with this easily accessible medium. There are increased opportunities for occupation, education, communication, development, entertainment, shopping, creativity, participation and civic engagement, social interaction, and connectedness [32–34]. Previous research has identified the many benefits of using ICT and the internet for users, including for those users with intellectual disabilities [35]. These benefits have been organized into themes such as social utility, accessing information, personal identity, and occupational and enjoyment. These themes were based on the users and gratifications framework [36, 37].

Table 5.1 Themes of the benefits of internet and digital technology usage with examples

Social and communication	• Communicating with other on social media, and other platforms • Developing and maintaining friendships and romantic relationships • Unity with family and friends
Cognitive	• Develop social learning skills • Learning about themselves, others, and other things
Occupational	• Employment • Education
Independence	• Online shopping • Online banking
Supportive	• Support groups and online discussion boards • (Mental) health information

Within this chapter, we will examine the benefits of internet and ICT usage for individuals with different mental disorders, and will organize the benefits into themes based on clinical impairments (DSM-5) such as, *social and communication, cognitive, occupational, and independence*. The additional theme of *supportive* is included due to the supportive benefits

the internet and digital technology provide to those with mental disorders (detailed in Table 5.1). Several of these themes can overlap each other, due to their related nature. For example, attending an educational institution online not only has occupational benefits but has cognitive benefits through learning as well as social and communicative benefits through communication with peers.

The supportive theme has been appended, as for many individuals with mental disorders, the services provided by interacting with the internet and the digital world have brought about many benefits to support those who would have found it otherwise difficult to find or receive help [38]. For instance, interacting with online message or discussion boards has been seen to reduce stress [39]. Furthermore, many individuals who engage with online support groups receive plentiful benefits, through being able to express themselves and their emotions, enhancing their knowledge, and maintaining family and friends' relationships [40, 41].

5.3.2 Risks of Online Interaction

There are many benefits of engaging with the online world. But, with these benefits also come several risks. There are two types of risks that online engagement can bring to individuals with mental disorders:

1. The risk of exacerbating the symptoms of the disorder,
2. The risk of becoming a victim of cybercrime.

Any user is vulnerable to cybercrime. However, do the symptoms of a mental disorder compound the user's vulnerability? To understand this, we will briefly discuss to which cybercrimes users are vulnerable.

There are many definitions of cybercrime, however, within this chapter we will use Nurse's definition and taxonomy of cybercrimes against individuals (2019), as it has been derived from a "comprehensive and systematic review" of research, practice, and real-world cases. Reference [42] defines "any crime (traditional or new) that can be conducted or

enabled through, or using, digital technologies". His taxonomy of cybercrimes against an individual includes five main types:

1. Social engineering and trickery,
2. Online harassment,
3. Identity-related crimes,
4. Hacking,
5. Denial of services and information.

Social engineering and trickery include phishing and catfishing. Through phishing, for instance, criminals aim to steal the user's confidential information such as authentication credentials (username and password), and/or online banking details [13]. The crime can occur when an individual overly shares personal information about themselves and others, and/or is willing to trust the sender and give them what they request in the communication, e.g., financial help. Criminals will often use techniques to get what they want, through claiming their issue is important and urgent, and presenting themselves in an official capacity, such as an organization, or someone of trust, like a potential partner. They often manipulate the victim in highly stressful situations and preying on anxieties where decision-making is not optimal [43].

Online harassment can occur when an individual has been too trusting with their personal information, and identity online. Through revealing their information, it can be utilized to direct anger and hate towards them. Examples of these types of crime include cyberbullying, stalking, and trolling [44]. The criminal uses the anonymity of the internet to act as they please harassing and manipulating the victim [45].

Identity-related crimes refer mainly to identity theft. It occurs due to the enormous amount of personal information that is available online. It can also be contributed to by a victim sharing personal information online, which is then extorted and used by the criminal in an anonymous environment to gain what they want. The criminal can also use the victim's

information to engage in further criminal activity [42].

Hacking can include compromising digital information and computing systems, targeting the cybersecurity principles of confidentiality and integrity [11]. Hacking can lead to the exposure of confidential information and/or modification and deletion of information. Hacking can occur through malware, such as spyware, and through account hacking by means of exploiting insecure password management behaviors (e.g., reusing passwords). Criminals exploit users' awareness (or lack of) regarding their security and privacy and their poor security behaviors, such as creating weak passwords, and reusing and modifying them for several accounts, due to convenience and memory burdening [46, 47].

Denial-of-Services (DoS) and information refers to when criminals will, for instance, bombard organizations with website traffic which can lead to genuine users being unable to access services or information [11]. Another type of crime can include ransomware, where the criminal will apply malware to encrypt an individual's (or organization's) information then request payment for the release of the information. Criminals will exploit the individuals' anxieties and manipulate them into getting what they want, as quickly as possible. These forms of crime target the cybersecurity principle of availability [42].

5.3.3 Cyber Security Behaviors

As mentioned in the previous section, there are many risks to being online and inter- acting with digital technologies. Cyber criminals attack individuals and organizations, and targets the basic principles of cybersecurity (CIA: confidentiality, integrity, and availability) [17]. There are technical protocols in place to attempt to prevent attacks and decrease the user's vulnerability, such as virus scanning software. However, the user still needs to undertake cybersecurity activities/secure behaviors to ensure they (as a vulnerable factor) are not the weakest link in security.

There are many security behaviors an individual can perform including [48, 49]:

- Securing their devices, systems, and services with good password management,
- Being careful with their privacy (i.e., not oversharing),
- Archiving and backing-up information,
- Virus scanning,
- Updating applications and software,
- Installing and updating security patches,
- Avoiding and not opening suspicious emails and websites,
- Not plugging in suspicious USB drives, etc.

We will discuss some of the main behaviors within this section.

Good or secure password management starts with creating a strong password.

Many users believe if the password is strong it is difficult to remember, but this is not necessarily the case. Passwords can be incredibly memorable as long as the individual has contributed the effort to make it so. Individuals can use memory techniques such as mnemonics to help them create strong passwords and to remember them as well [46, 47, 50]. However, creating a secure password is not all about making it strong and meeting the minimum password policy requirements [51, 52]. A strong (long and character-complex) password can be broken if the individual uses the password for many accounts, where the security-levels of some systems are not as strong. Or, the individual uses predictable patterns, such as “Cappuccino1!” and “Cappuccino2!”, modifying their passwords for several accounts, that hackers can exploit [53]. Other insecure password behaviors include writing passwords down in an insecure (or not encrypted) document or post-it note, and sharing passwords. Many users adopt these behaviors for two main reasons: convenience, and memory

burden. Users are not willing to expend the time and effort into creating strong passwords, and when there are so many accounts, many feel overwhelmed by how many passwords they would be required to create, learn and recall. Therefore, they adopt insecure password behaviors and undermine the authentication mechanism [14].

Oversharing and disclosing personal information and carelessness with privacy can result in the individual being vulnerable to most cybercrimes. It can lead to exposing details of not just the individual but others around them, and organizational information. For instance, in one case, people were using fitness trackers to track their exercise patterns and unintentionally revealed details of a military base as they posted their results to an online application [54]. Through trusting and sharing personal information online, this can unintentionally expose details that allow criminals leverage to manipulate the individual into doing what they want them to do.

Proactive security behaviors include, virus scanning, updating applications, and software, installing and updating patches that require very little effort, as the technology does the work for the individual [55]. All the individual is required to do is regularly remember to start the action (often when prompted) and give the system time to undertake the process. Some users do not undertake these activities due to the inconvenient time when they are required, or because updates may change the application to a less user-friendly version, or because they are unaware of the risks of not taking these actions [56]. Individuals who exhibit risk-taking behaviors have been found to be less likely to undertake these proactive security practices [57].

Backing-up data and information: losing data is common among individuals and organizations, however, using backup solutions can prevent the threat of losing data [58]. Backup solutions include cloud solutions, and external hard drives, and USB sticks. If data is not backed-

up it can be impossible to recover if an incident occurs. Regularly backing-up data can ease the burden of data loss in the event of accidental deletion, intentional deletion through malware, hard drive crash, power failure, or a natural disaster [59]. As seen with updating virus software, applications, and patches, backing-up data does not require much effort, however, users contemplate the perceived convenience over perceived threat [58].

Not opening suspicious emails, clicking on suspicious links, or visiting suspicious websites: users can be encouraged to do these actions through social engineering by the medium of phishing emails. A prime example can include, when users receive a scam email and are invited to visit fraudulent websites. The criminal creates a website that is designed to look like an official legitimate website. The user is asked to enter their authentication credentials for a service, they may already use. The criminals can then access the victim's account, potentially other accounts (if their passwords are reused), and use the details for other criminal activity [13, 42, 53].

Using personal USB drives within organizations, and using suspicious USB drives can bring a whole host of security threats to an organization or to an individual. Many users do not have as strict cybersecurity practices at home, with insecure networks. The user will plug-in their USB drive at home, picking up e.g., viruses, then bring it to work and spread the viruses [18]. Another issue comes from users being given USB drives for free (sometimes as a marketing promotion), or just finding them. Criminals will leave USB drives for individuals to find in the hope they will just use them—and they do. These drives are often full of malicious software to allow the criminals to gain access remotely to secure systems [11, 60].

For many years, it has been acknowledged that psychology plays a role in the adoption of security and protective practices by the users. However,

very few studies have considered the role that psychopathology plays in users' safety behaviors and interaction with cybersecurity.

5.4 Understanding Users' Mental Disorders

This section describes some of the major classes of mental disorders with reference to DSM-5 [29]. Eight of the 19 major classes are reviewed. They were chosen due to their prevalence in society and relevance to online interaction. Substance-related and addictive disorders will not be discussed in this chapter. This is because the recognition of internet-based disorders (named currently as internet gaming disorder) represents excessive internet abuse [24, 29] and is classified under this major class. Owing to the growing phenomena of internet-based disorders, a separate chapter would be required to fully review them.

Therefore, using the characteristics of eight classes of mental disorder, the benefits and risk to online interaction will be considered. These characteristics will be applied to the context of cyber security to reflect upon the vulnerabilities to cybercrimes that individuals with these disorders may face and how their disorder traits influence their cybersecurity behavior. Finally, a summary of mental disorders is presented.

5.4.1 Neurodevelopmental Disorders

Neurodevelopmental disorders are a group of disorders that occur during the developmental stage. They are characterized by developmental impairments that vary from specific limitations in learning and in controlling attention to more general impairments in intelligence and social skills. These disorders usually manifest in the early stages of development, usually before a child goes to school. With this early onset, these disorders with a variety of impairments often cause limitations to personal, social, or academic performance. Neurodevelopmental disorders

class includes intellectual disabilities, communication disorders, autism spectrum disorder, attention-deficit/hyperactivity disorder (ADHD), and specific learning disorder [29].

Intellectual disabilities are characterized by significantly impaired intelligence, deficits in general mental abilities, and impairments in everyday adaptive behavior. Communication disorders are characterized by difficulties in speech, language, and communication. They have not always been considered as mental disorders. However, the impairments can cause distress and limit functioning in life, and there- fore are now considered as disorders. Autism spectrum disorder is described as a disorder with symptoms that are persistent deficits in shared or common social communication. It is accompanied by nonverbal communicative behaviors used for social interaction, impairments in developing, managing, and understanding relation- ships, and restricted, repetitive patterns of behavior, interests, or activities. ADHD, on the other hand, is categorized by inattention, and/or excessive activity and impulsivity which can interfere with development and functioning [61], which is not appropriate for the individual's age. Specific learning disorder is characterized by learning difficulties and difficulties in applying academic skills accurately or as quickly as others of the same age. It is more commonly known as the reading disorders such as dyslexia and dyscalculia.

All these disorders can be generally categorized to describe them. However, they will vary in numerous impairments and in their severity. For instance, some individuals may be able to interact and function in society, however, others are affected enough by symptoms such as inability to critically think, lack of foresight, or a delayed response to all information processing; this makes interaction incredibly difficult in society (McHale, 2010). Additionally, more than one neurodevelopmental disorder will frequently occur. For instance, individuals with autism spectrum disorder will often have intellectual disabilities, and many

individuals with ADHD will also have a specific learning disorder [29, 30, 62].

Through interacting with the online world, this can afford many benefits but also brings about risks to individuals with neurodevelopmental disorders. The online world provides an environment where individuals can engage and develop relation- ships, learn and develop their social skills, and learn about themselves and others. It allows many to communicate with many others, providing a platform that can encourage self-expression more easily, often due to anonymity or being physically distanced [63]. In addition to the social and cognitive benefits of engaging with the internet and digital technology, it can also provide occupational and supportive benefits such as employment and education, online health (and mental health) information, online therapies, and support groups. These can be particularly useful as social engagement can be challenging for many individuals. Furthermore, digital technology can also allow many to become more independent, accessing entertainment, services, online shopping, and banking, and provide assistive technologies if required [35, 64–66].

However, regardless of the benefits the internet and digital technology afford users there are many risks for users with neurodevelopmental disorders. Individuals with these disorders can lead to maladaptive use of the internet [23], due to issues regarding critical thinking and judgment [66]. Individuals with neurodevelopmental disorders can also be vulnerable to cybercrime, dependent on the disorder and severity of the disorder. These may include being cyberbullied and harassed [35, 67], and being vulnerable to scammers, social engineering, privacy risks, and account hacking through errors in judgment and/or reading, or misunderstandings.

Individuals with neurodevelopment disorders may have significant challenges with performing cybersecurity behaviors. When creating strong

passwords, individuals require intelligence, attention, and learning skills. Those with intellectual disabilities, specific learning disabilities, and ADHD may find it particularly difficult to create and learn strong passwords, and therefore, may adopt insecure password behaviors such as reusing passwords. Those with autism spectrum disorder may also find difficulties coping with different password strength requirement policies due to inflexible thinking patterns, which could lead to frustration and stress. Disclosing and sharing information and personal details, as well as opening suspicious emails and websites, may bring about cybercrimes upon individuals without critical thinking, awareness, and judgment. These characteristics can be present in individuals with intellectual disabilities and autism spectrum disorder.

Virus scanning, installing and updating applications, software, and security patches, and backing-up data often require minimal action. However, those who lack judgment and awareness, may ignore any cues to perform these actions. Individuals with specific learning disorder (i.e., dyslexia) often make errors when reading text. Therefore, they may also make errors when reading scamming emails, leading them to click on suspicious links and disclose personal information as a result. These errors increase their vulnerability to crimes such as hacking and identity theft. They may also fear and experience anxiety updating applications and software due to the worry of making such reading errors.

5.4.2 Schizophrenia Spectrum and Other Psychotic Disorders

Schizophrenia spectrum and other psychotic disorders include schizophrenia, other psychotic disorders, and schizotypal (personality) disorder. They affect more than 20 million people [68] and are characterized by positive and negative symptoms.

Positive symptoms include abnormalities in one or more of the

following areas: delusions, hallucinations, disorganized thinking (speech), disorganized or abnormal motor behavior. Delusions are fixed beliefs that the individual has and is not willing to change even when faced with contrary evidence. They can include such beliefs:

- the individual will be harmed in some way by anyone or anything;
- the individual has exceptional abilities or is famous;
- another individual has negative or positive emotions towards them, such as love;
- concern about a major event occurring;
- preoccupation with their health.

They are often considered weird or bizarre as they are obviously not conceivable in most people's lives. Hallucinations are experiences perceived by the individual without any external stimulus. They can include all senses, however, auditory hallucinations are the most common, such as hearing voices. Disorganized thought is often represented through speech, where the individual will switch or jump from topic to topic with loose associations during one conversation. Disorganized motor behavior can manifest ranging from child-like behavior to unpredictable agitation to catatonia. Negative symptoms on the other hand, are represented by the absence of emotions and behaviors, such as becoming withdrawn, unmotivated, or unresponsive [29]. Individuals with these disorders will experience phases of positive and negative symptoms, of which these phases can last for varying periods of time.

These disorders are considered to be severe, with the individual becoming disassociated from reality and potentially dangerous. In situations when they become a danger or risk to themselves or to others, this will lead to periods of hospitalization [69]. The disorders vary in occurrences dependent on factors such as gender, and economic status [70]. Although they have a genetic component, it is often the environmental factor that triggers the disorder or episode, such as stress,

drug-taking, and alcohol abuse.

Due to the severity of the schizophrenia spectrum and other psychotic disorders, it is difficult for many to interact with the online world in a positive manner. However, there are some benefits through engaging with the internet and digital technologies such as social and communication, supportive, and possibly independence (dependent on severity). For those, especially while experiencing the negative symptoms (if they are not in a catatonic state), may be able to communicate with others and interact with society over social media and chatrooms. They may be able to also use services such as online shopping, and entertainment, providing some sort of level of independence. Supportive services can also be accessed including support groups, health information, and therapies.

The risks of online interaction arise when considering the positive symptoms of these disorders (if they are able to interact at all). When an individual experiences positive symptoms, they are evaluated for hospitalization based on whether they are considered a danger or risk to themselves or others. These positive symptoms can be transferred to the online world if they are able to interact with technology. Therefore, engaging with the internet can pose a risk to themselves, and they can pose a risk to others through the medium of the online environment. Examples of how interactions with the online world can become a risk to the individual can involve finding information (real or fake) that could support delusional thoughts, such as conspiracy theories [28]. Owning digital technology such as a smartphone, or smartwatch can lead to paranoia and delusions of being monitored, and privacy being invaded. Furthermore, through the increased stimuli that engagement with technology and the internet provide, this can also increase the likelihood of hallucinations, where the individual may believe that, for example, a blogger may be talking about them, or directly to them. In addition, due to impaired and disordered thoughts and delusions, individuals with

schizophrenia spectrum and other psychotic disorders are more likely to be vulnerable to cybercrimes, including bullying and harassment, social engineering and scamming, identity theft, and hacking. On the flip side, these disorders can present themselves through maladaptive behavior, and exhibiting intense and unpredictable emotions including, anxiety, aggression, and may even lead to violence—becoming a danger to others [29]. If the individual is able to interact with technology and the online world, they may also become a risk to others. This can involve, creating fake news online, posting offensive or unacceptable information generally directed, or directed at a specific person, participating in online harassment and even cyberstalking, and inciting hate crimes in others, all as a result of delusions.

Engaging with cybersecurity may prove difficult for those individuals with schizophrenia spectrum and other psychotic disorders. With positive symptoms, if the individual is able to interact online, creating and learning strong passwords may not be of concern, if the individual has other goals in mind. Disorganized thoughts may prevent the individual from engaging with any type of password management, which may prevent them from gaining access to online services and accounts. On the other hand, not being able to remember passwords while experiencing positive symptoms may influence them to create weak passwords, or write passwords down, while in a more lucid state. As a result of disorganized thoughts and decreased judgment, these individuals may divulge personal information about themselves and others online, be more willing to plug-in devices, and more easily coerced into clicking on suspicious links and visit suspicious websites, which increases the risk of becoming a victim of cybercrime. While experiencing negative symptoms, individuals may avoid or forget to update software, applications, and patches, again leaving them and their technology potentially open to attacks.

5.4.3 Bipolar and Related Disorders

Bipolar and related disorders bridge the main classes of schizophrenia spectrum and other psychotic disorders and depressive disorders, due to the presence of symptoms from both classes. They include a range of disorders associated with bipolar, such as bipolar I disorder, bipolar II disorder, and bipolar induced by substances, medication, or medical conditions [29].

Bipolar I disorder refers to what many would know as classic manic-depressive disorder, whereas bipolar II is a milder version. The disorders are characterized by swings of extreme emotional highs, manic symptoms, and psychosis to major depressive episodes. During manic phases, an individual can experience excitable moods, endless energy, and increased appetites. Often the individual will feel as they do not need sleep and may binge on food, alcohol, drugs, and sex, and undertake risky behaviors. During the depressive stage, individuals will experience periods of major depression, feelings of hopelessness and guilt, suicidal thoughts, and increased sleep [30]. The different episodes can last weeks and have a significant impact on the individual's life, as they find it hard to manage the extreme moods.

The different stages of bipolar disorders may lead to different ways in which an individual will interact with the online world. The benefits of online interaction can provide social engagement and communication, support and health information, and independence during both manic and depressive stages [71]. During the depressive stage, social interaction and communication can help create a support network for those individuals that may have found it hard to interact without access to the internet. Online therapy, support groups, can also aid individuals during manic stages (ibid.). Furthermore, the availability of services such as online shopping can provide levels of independence to users as well.

Problems occur, mainly through the manic stages when access to the internet can become detrimental, as with schizophrenia spectrum and

other psychotic disorders, the maladaptive behaviors are transferred to the online world. Individuals experiencing a manic stage often exhibit risk-taking behaviors, not fully aware of the danger they may be putting themselves in. Risky online behaviors can include, excessive online shopping, online gambling, and engaging in cyber sexual behavior (e.g., sexting, engaging with strangers online, and visiting suspicious sexual websites) that could result in dangerous situations [28]. As the manic individual often finds it hard to sleep, the 24/7 availability of the online world provides the perfect environment for several cyber risks to manifest, especially when the individual lacks self-control. Although most risks from online interaction can be seen during the manic stage, there are some during the depressive stage too. Many might feel more acutely isolated when they view the social world online and are not engaged with it. Moreover, if the individual is cyberbullied or becomes a victim of other cybercrime, this may fuel their feelings of desperation leading to suicidal thoughts.

The different stages of bipolar disorders can affect how the individual will perform cybersecurity behaviors to protect themselves. During a manic stage, the individual may not be concerned with creating and learning a strong password when their goal is to gain access to, for instance, an online gambling website. They may also have issues with recalling passwords due to their manic unstructured thoughts. Moreover, the depressive stage may affect the motivation to engage in secure password behavior and result in forgetting passwords. These issues may lead to choosing convenience over security with regards to password management. Individuals experiencing a manic stage may also be more willing to share private information and be more easily manipulated to reveal further information, and agree to criminals' demands. These symptoms may also result in clicking on dubious email links and websites, and using suspicious USB devices. With risk-taking behaviors as a common trait in these individuals, users are less likely to perform

proactive security behaviors, such as virus software updates [57], and the likelihood of circumventing security policies and protocols are more likely, increasing the risk of being a victim of cybercrimes.

5.4.4 Depressive Disorders

Depressive disorders are one of the most common types of mood disorders [31]. 264 million people are affected by depression, with more women being affected than men [68]. There are many depressive disorders including the most commonly known, major depressive disorder (MDD). The most common symptoms are the presence of sadness, emptiness, irritable mood, a loss of pleasurable feelings, and interests, physical slowness, social withdrawnness, loss of appetite and weight gain, and many more. This can be accompanied by somatic symptoms and cognitive impairments. Somatic symptoms include physical aches and pains, whereas cognitive impairments can include, lack of concentration, and learning and memory impairments. The episodes of symptoms can vary in intensity and duration, and can significantly affect the individual's capacity to function impeding on social and occupational functioning [29].

With depressive disorders, there are many benefits from engaging with digital technology and the internet. Many individuals often withdraw into themselves and avoid contact with others. Therefore, the online world provides them with a platform to interact in social activities and communication. However, they may still not choose to engage in these activities as their symptoms are too severe. Nevertheless, they are able to gain support through online mental health information, participate in support groups and receive therapy, if they are able [72]. Due to the symptoms of depression, individuals may still not participate with supportive online interactions for reasons such as, not believing it will help [73, 74]. They are also able to continue to be independent, as when individuals feel unable to, for example, leave the house, they are able to

continue to shop, bank, and even undertake work and education online, maintaining their independence.

The risks of individuals with depressive disorders being online are synonymous with those with the depressive stages of bipolar disorders. Viewing the world through the lens of technology can increase the feeling of isolation, which can exacerbate their symptoms further. Similarly, if the individual becomes the target of online harassment, this can also worsen the symptoms [75], and potentially lead to suicide. Furthermore, through their cognitive abilities slowing, this can result in mistakes that can increase the likelihood of becoming a victim of other cybercrimes, such as hacking and identity theft.

Individuals with depressive disorders are often distracted and consumed by their symptoms, accompanied by the slowing of cognitive processes [30]. This could lead many to not consider cybersecurity too much and becoming passive towards any cues of criminal activity or attack. Moreover, due to memory impairments, the individual may find it difficult to remember passwords, and therefore adopting insecure password behaviors (reusing, writing passwords down, etc.) to continue to allow access to systems, devices, and services. Slowness in cognitive processing may lead to impaired decision-making, resulting in individuals clicking on suspicious links, and visiting dubious websites, and poorly evaluating the security of their actions [76]. Furthermore, the memory impairments could also lead to passive inactivity regarding software, application, and security patch updates, all resulting in increased vulnerability.

5.4.5 Anxiety Disorders

Anxiety disorders are the most prevalent of mental disorders, with over 284 million people affected globally [68]. As with depressive disorders, most people experience at some time in their life, a bit of anxiety.

However, the difference between “a bit” and a disorder is determined by the severity—is it severe enough to disrupt a person’s everyday life and functioning? There are a variety of anxiety disorders, for instance, generalized anxiety disorder (GAD), separation anxiety disorder, social anxiety disorder, panic disorder, substance/medication-induced anxiety disorder, and more. They all share characteristics of excessive fear and anxiety, and related behavioral disturbances. The DSM-5 defines fear as “the emotional response to a real or perceived imminent threat”, whereas it defines anxiety as “anticipation of future threat” ([29], p. 189). Although they are similar, there are some distinctive differences, for example, fear often activates the fight or flight autonomic mechanisms, with thoughts of immediate danger, and strategies and resulting escape behaviors. Anxiety often leads to alertness, preparing for a future threat, resulting in muscle tension, cautiousness, and even avoidance.

Many individuals experience panic attacks with their anxiety disorder as a specific response to fear. However, panic attacks are not only experienced by those who have an anxiety disorder, they are also present with other mental disorders. Like with many mental disorders, there are genetic factors that are often triggered by an environmental factor such as stress.

Generalized Anxiety Disorder (GAD) is one of the most common anxiety disorders and is characterized by frequent, persistent excessive, and uncontrollable worry and anxiety that is often irrational or more excessive than the object of worry warrants [30]. Many individuals also experience feelings of panic, paranoia, and can suffer from paralysis, stimming, stuttering, their mind going blank, and adopt avoidance behaviors. Individuals may also experience bouts of depression [29]. Many people who have never experienced an anxiety disorder may ask, “but why do you feel anxious, what triggered it?” Yet, sometimes the initial trigger may have occurred several years ago, and since then the anxiety persistently occurs with no event or reason and reoccurs with no warning.

In many cases, the anxiety and worry are often severe enough that they will impede on the individual's social and occupational functioning.

The benefits that an individual with Generalized Anxiety Disorder (GAD) will gain through interacting with digital technology and the online environment are plenty. Where individuals with GAD would possibly withdraw from society due to their symptoms of social anxiety, the online environment provides a means to engage with society and communicate with people through social media platforms, etc. It allows these individuals to express themselves while still being able to socially distance [77]. Whereas, leaving the house for shopping or going to work/education, or attending a therapy session could prove difficult for many, accessing these services online improves their quality of life [72]. However, being able to access life via the online world instead of the offline world can enable the individual to avoid the actual issue. Furthermore, even though the individual can interact online, the symptoms do not disappear. This means their thoughts and behavior can be transferred online. Many may feel anxious about being misunderstood [77] through the lack of personal or e.g., visual interaction. Many may interpret conversations from others differently to their intended purpose, which could exacerbate their symptoms. They may feel overwhelmed by the amount of communication, avoid important communication as well as worry about not replying immediately. Some individuals may develop a phobia towards technology and feel paranoid towards technology monitoring and invading their privacy. Some individuals could feel paranoid or worried that they are missing out, and feel depressed viewing society continue without them participating [78]. Symptoms can also be triggered or increased through others gaining too much access to the individual when all they want to do is withdraw and recover but feel pressured to interact. Individuals with GAD are also vulnerable to several cybercrimes, such as social engineering [79] and DoS ransomware

attacks, where the criminal can manipulate them preying upon their insecurities and anxieties. They can also be severely affected by cyberbullying and harassment, which can intensify their symptoms [75].

Cybersecuritybehaviorcanbeaffectedbyanxietydisordercharacteristicsin many ways, dependent on the type and severity of symptoms. If the individual is more anxious, they could perhaps be more cautious with their security and privacy? This may be the case for some, however, through the worry and fear of cybercrimes and attacks, and becoming a victim, it can become counterproductive. For example, individuals who are more anxious about remembering their passwords, often adopt insecure password behaviors such as password reuse to compensate for their perceived memory capabilities [80]. Some individuals who suffer with anxiety, and worry about their cybersecurity, may install several antivirus software programs ("just in case"), which can often end up working against each other, causing the individual's computer to be vulnerable to attacks. In addition, to the lack of security, having these programs operate at the same time, slows the computer and can overload it when updates are required. This further leads to potential loss of data. What is more, individuals with anxiety disorders such as GAD can often be consumed and preoccupied (as with depressive disorders) with their suffering and with very little thought for cybersecurity, leading to errors in judgment such as clicking on suspicious links in emails. Individuals can also become easily overwhelmed, by too much contact with others, too much information to process, and complex information, which leads many to ignore communications and adopt avoidance behaviors. Through becoming overwhelmed and resulting in avoidance, the individual may not recognize or acknowledge warnings or cues that their cybersecurity is being threatened (e.g., security warnings or messages to update patches), and may become inactive in protecting themselves and their systems.

5.4.6 Obsessive–Compulsive and Related Disorders

The class of obsessive–compulsive and related disorders include several disorders such as obsessive–compulsive disorder (OCD), body dysmorphic disorder, hoarding disorder, trichotillomania (hair-pulling disorder), excoriation (skin-picking) disorder, and substance/medication-induced obsessive–compulsive and related disorder. Obsessive–compulsive disorders are more common than many realize, experience by about 2% of the global population, and are considered one of the top causes of disability [20]. Obsessive–compulsive disorders have common characteristics including obsessions and/or compulsions. DSM-5 [29] defines obsessions as "recurrent and persistent thoughts, urges, or images that are experienced as intrusive and unwanted". Whereas, they define compulsions as, "repetitive behaviors or mental acts that an individual feels driven to perform in response to an obsession or according to rules that must be applied rigidly" ([29], p. 235). Other obsessive– compulsive disorders can also show the presence of symptoms of preoccupations and repetitive behaviors or mental acts in response to the preoccupations. Some of the obsessive–compulsive disorders have characteristics with recurrent body-focused repetitive behaviors, such as hair pulling, and skin picking, with repeated attempts to decrease or stop the behaviors [29].

With OCD, the obsessions and compulsions can vary in each individual. However, there are many common themes to the obsession-compulsions such as cleanliness, forbidden thoughts (e.g., sexual, violence, etc.), symmetry, harm and death. The intense anxiety that accompanies the obsession, with the repetitive thoughts can be extremely distressing and often lead to compulsive repetitive actions [30]. The thoughts can be rational, for example, not washing your hands after being in public, could potentially result in catching coronavirus, leading possibly to death. However, sometimes the thoughts are irrational, and even though the individual may understand they are irrational, the fear of the outcome may

be too overwhelming to deal with. For example, worrying thoughts of not turn the light on and off five times will result in losing your job. The individual may know they will not lose their job but will do the repetitive behavior anyway, just in case. In really extreme circumstances, the behavior can lead to washing hands until they bleed, acting out dangerous behaviors, such as walking in front of cars, or on the other hand, protective behaviors such as saving data in many forms of back-ups, and never throwing anything away. OCD, like most psychological disorders, is genetically based but requires an environmental trigger. Triggers can include, abuse experienced as a child, or a traumatic event such as abuse, bullying, a death, or loss of some kind.

Interacting with the online world can bring benefits to individuals who have OCD. Like with anxiety disorders, individuals can communicate and socially interact with others and society in general through social media, and platforms. They can get access to services, for instance, news outlets, online shops and banks, education, and work. Many can also express themselves and their thoughts anonymously through the medium of the internet, where they may feel more comfortable. In this way, they can gain access to support through groups and therapy [81].

Nevertheless, the online world poses risks as well as benefits. As with anxiety disorders, the ability to enact many life functions through the medium of the internet can result in individuals ignoring the issues they have and not seeking help or treat- ment. Using the internet and digital technology can also fuel these disorders, through filter bubbles and personalized internet searches presenting individuals with what they want to see, even if it is fake news—giving them an unbalanced and potentially dangerously biased view [82]. If an individual with OCD is concerned about their health, the effects of personalized search results can fuel their worry. Fake news, privacy invasion, and worries around technology monitoring can also fuel an individual's disorder. Individuals with OCD

can become victims of cybercrimes. Cyber- bullying, hacking, and social engineering. With the compulsion being the motivation behind an action, this allows cybercriminals to manipulate individuals, preying upon their anxieties, and their obsession in completing their behavior.

When experiencing symptoms of OCD, many feel compelled regardless of the result or cost to enact a behavior to appease the obsessive thoughts. Two themes that can be common amongst those with OCD are hygiene/cleanliness and protection as a response to the threat of potential harm [29]. These themes could potentially lead to more proactive security behaviors [43]. However, the behavior can eventually become more extreme, turning counterproductive. For example, the individual may be less trusting and hypervalent, being careful to not open suspicious emails or click on unknown links, but, if a thought arises in their mind that they have to do these actions, they will probably do them. Another example can include, zealous but rational protective thoughts can result in cybersecurity issues, as with anxiety disorders—overcompensation leading to, e.g., antivirus software working against each other. Moreover, irrational thoughts, such as, *my friend might die if I do not uninstall the antivirus software* will also lead to vulnerability. All cybersecurity behaviors could be potentially affected in the same way, as with anxiety disorders it will depend on the severity and type of issues that the individual has, which will deter- mine how they interact with cybersecurity. Individuals with OCD could potentially have problems with managing their passwords. Issues such as choice of password could potentially be a problem, as the choice may come from preference from an obsessive thought, and not protection, e.g., *will choosing 1 or 2 result in death* (or other outcomes)*?* The individual may become fixated with a specific password and reuse it for many accounts. However, when a password policy requires other criteria, this may lead to frustration, anger, and anxiety. These issues lie with the motiva- tion behind the behavior—even if the theme is protection, the

behavior is driven by a compulsion rather than protection itself. Therefore, individuals with OCD can leave themselves open and vulnerable to attack from all types of cybercrime, and manipulation from criminals.

5.4.7 Neurocognitive Disorders

There are several neurocognitive disorders (NCDs), however, they can be divided into three subtypes, delirium, major neurocognitive disorders, and mild neurocognitive disorders. Delirium refers to a notable decrease in awareness and attention. Major and mild NCDs include disorders that are caused by diseases such as, Alzheimer's, Parkinson's, Huntington's disease, HIV, and from traumatic brain injury, etc. Neurocognitive disorders are symptomatic of changes in the brain structure, function, or chemistry [30]. Although many mental disorders include cognitive impairments (e.g., memory impairments in depression), NCDs are disorders where cognitive impairments are the main characteristic. Furthermore, they are not present since birth or since early life, and therefore, represent a decline from "normal" functioning. NCDs can include cognitive impairments such as complex/divided attention (e.g., paying attention within an environment with many stimuli, for instance holding a conversation and the TV playing at the same time), planning or decision making, illogical thinking, learning, and recalling, using language, and social cognition (e.g., knowing how to behave in different settings). When cognitive decline occurs, it may not only impact upon the individual's life, socially, occupationally and with everyday functioning, it can also be frightening, and frustrating [29]. Furthermore, the individual often requires levels of care from family, friends, and/or professionals due to the inability to undertake everyday activities, and/or be trusted to be able to care for themselves.

Digital technology and internet access can provide many benefits for individuals with NCDs in terms of social and communication, cognitive,

occupational, supportive, and independence benefits, depending on their levels of severity [83, 84]. Individuals can establish and maintain social relationships online using social media. They can also find information online when they have forgotten particular information. They can interact with work and education if they are able. Digital technology and the internet are most useful when considering support and independence [85]. Through being more in control of their lives, through access to online services, including banking and shopping, can empower an individual with NCDs, whereas previously, an appointed carer would do these things on their behalf [83]. If the individuals are at the stage of their disorder where a carer is needed, the individual will obviously not be able to engage with the online world fully and therefore would not receive all the benefits of being online. However, digital technology and the internet can support the carer in their role as a caregiver [86]. Nevertheless, individuals with NCDs can gain access to telecare or telehealth [87], providing care, therapies, and support groups remotely. Participation and exchanging issues around symptoms with those who are in similar circumstances can lead to various positive outcomes [88]. Furthermore, with developments in technology, assistive technologies have allowed many to live independently in their homes. Specifically, assistive technology, an umbrella term refers to any device or system that allows an individual to perform a task they would otherwise be unable to do or increases the ease and safety with which the task can be performed [89]. Personal assistants in the form of mobile devices, aid those individuals that have memory impairments, with their contacts, to-do lists, and schedules [90]. Furthermore, cognitive agents are AI that resolves issues that individuals may have when interacting with technology, such as reformatting screens and enhancing relevant information when the individual has attentional impairments.

Digital and internet interaction pose many benefits for users with NCDs,

however, there can be issues, if the individual has no close family or friends who are internet users. This can present the problem of getting the help and guidance they need to interact with digital technology and in the online world. Until recent times, security risks were often mitigated through avoidance—an assigned person (family member or carer) would interact online with accounts and services on the individual's behalf. However, nowadays with assistive technologies, more individuals with NCDs are able to go online, and therefore, be at a higher risk of exploitation and vulnerability. Individuals with these disorders are potentially vulnerable to cybercrimes, such as social engineering, identity theft, and risks to privacy, because of attentional and memory impairments, and confusion over knowing who and what to trust, and illogical thinking.

Individuals with NCDs could find password authentication particularly difficult to manage, as the cognitive impairments related to attention and memory would make it incredibly difficult to create, learn and recall strong passwords. This could potentially lead many to adopt insecure password behaviors, and susceptible to hacking. Over- sharing personal information, opening suspicious emails, and clicking on dubious links and websites may also become problematic through individuals not knowing whom to trust or possibly not knowing with whom they are talking or interacting. This will leave them especially vulnerable to social engineering and scamming. With regards to proactive security behaviors such as virus scanning, software updating, etc., the individual with NCD may be confused by the security messages and cues to take action and forget to do so. All of these may result in exposure to attacks.

5.4.8 Personality Disorders

Personality disorders have a general definition, and criteria that need to be met before applying one of the 10 specific personality types. DSM-5 defines a personality disorder as "an enduring pattern of inner experience

and behavior that deviates markedly from the expectations of the individual's culture, is pervasive and inflexible, has an onset in adolescence or early adulthood, is stable over time, and leads to distress or impairment" ([29], p. 645). Maladaptive traits and patterns of behavior, cognition, and inner experience are present across many contexts within an individual's life. The variety of traits has led to defining differing disorders. Although they may vary in some respects, they are similar in others.

These similarities have resulted in disorders being grouped into three clusters:

Cluster A: Paranoid, schizoid, and schizotypal personality disorders. Individuals with these disorders will seem eccentric or odd to others.

Cluster B: Antisocial, borderline, histrionic, and narcissistic personality disorder. Individuals with these disorders can appear erratic, dramatic, or emotional.

Cluster C: Avoidant, dependent, and obsessive-compulsive personality disorders. Individuals with either of these personality disorders may seem as fearful or anxious.

Details of each personality disorder are represented in Table 5.2. Dependent on which type of personality disorder an individual has will depend on how they are affected and the impact it has upon their life. For instance, an individual with paranoid personality disorder may find it difficult to have or keep an occupation or function within society due to symptoms of distrust and suspiciousness of others.

Table 5.2 DSM-5 [29] brief description of each personality disorder

Cluster A	Paranoid personality disorder	Pattern of distrust and suspiciousness such that others' motives are interpreted as malevolent

	Schizoid personality disorder	Pattern of detachment from social relationships and a restricted range of
	Schizotypal personality disorder	Pattern of acute discomfort in close relationships, cognitive or perceptual distortions, and eccentricities of behavior
Cluster B	Antisocial personality disorder	Pattern of disregard for, and violation of, the rights of others
	Borderline personality disorder	Pattern of instability in interpersonal relationships, self-image, and affects, and marked impulsivity
	Histrionic personality disorder	Pattern of excessive emotionality and attention seeking
	Narcissistic personality disorder	Pattern of grandiosity, need for admiration, and lack of empathy
Cluster C	Avoidant personality disorder	Pattern of social inhibition, feelings of inadequacy, and hypersensitivity to negative evaluation
	Dependent personality disorder	Pattern of submissive and clinging behavior related to an excessive need
	Obsessive–compulsive personality disorder	Pattern of preoccupation with orderliness, perfectionism, and control

Many individuals who have personality disorders may be unaware of even having the disorder and can be unaware of the way their thoughts and behaviors affect their own lives or the lives around them. This can be apparent with obsessive–compulsive personality disorder when compared with obsessive–compulsive disorder. With OCD the individual has recurrent thoughts that cause anxiety until the compulsions or behavior are untaken to relieve the obsessional thoughts. With obsessive–compulsive personality disorder, the individual engages with obsessive behaviors but is not necessarily anxious about their thoughts, only frustrated if they cannot complete the behavior. Many individuals with personality disorders are unaware that their thoughts and behaviors are not considered “normal”

by others. Many find that others around them do not respond to what they say or how they behave in a manner they expect. However, they do not understand why, but do not necessarily question their own abnormal or maladaptive behavior.

Users with personality disorders (regardless of the type) will benefit to varying degrees from interacting with digital technologies and the online world. This includes social and communication—individuals will be able to communicate through social media, engage with society, and can interact with friends and family. Cognitive benefits can be represented through individuals being able to express their emotions to others, and potentially anonymously if they felt more comfortable. Individuals whose disorder impedes upon their daily functioning may benefit occupationally through interacting with employment and education online. So too, with online shopping and banking, etc., allowing those to live independently. Finally, the online world can also provide support for those with personality disorders, offering health information, support groups, and online therapy.

The type of personality disorder and the severity of the disorder will affect the risks that online engagement will pose to the individual, and so too, the risks the individual will pose to the online world. This is also the case for the interaction with cybersecurity, as the individual may undertake risky security behaviors, and therefore, be vulnerable to attack. Although at the same time, they may undertake behaviors that could violate the cybersecurity of others. These will be discussed per personality disorder type.

Paranoid Personality Disorder

Individuals with this type of disorder could potentially be less likely to become a victim of cybercrime. Due to the suspicious nature and distrust of others, they are more prone to being hypervigilant towards their environment [30, 43], and less likely to overshare personal information

increasing the chances of social engineering, hacking identity theft, or harassment. However, many become hostile and aggressive in response to their paranoid thoughts and find conspiracies everywhere to support their paranoia. This could result in the individual becoming a cybercriminal by posting or messaging offensive information towards society in general or towards a specific person, by cyberstalking, by creating fake news, or re-sharing fake news. If they have the skills, they could hack accounts and systems seeking out information to confirm their paranoid beliefs. Regarding their cybersecurity behavior, individuals with paranoid personality disorder may adopt more secure password behaviors due to their paranoia and hypervigilance. They may also perform proactive security behaviors such as virus software updates, back-up files and data, and updating applications.

Schizoid Personality Disorder

Individuals with this disorder could possibly be less likely to be a victim of some cybercrimes such as social engineering and harassment. This could because they are often solitary, do not have many (if at all) close relationships, and find it hard to form meaningful relationships [29]. They tend to not experience strong emotions and therefore, do not have the need to express them. This means that individuals with this type of personality disorder may be less present (or not present at all) on social media sites and would not be sharing their opinions or views online, which decreases the likelihood of becoming a victim of those specific cybercrimes. These individuals if they were to experience cyberbullying, may also be less distressed by this type of crime due to their indifference to criticism. They may although, still be vulnerable to other cybercrimes, for example, identity theft, hacking, and denial of services, especially if they adopt poor security practices. However, these individuals are emotionally restricted and are not risk-takers by nature, and therefore, they may perform proactive security behaviors, be less likely to click on

suspicious links, back- up their information [57], and have good password management through the lack of emotive decision-making.

Schizotypal Personality Disorder

Individuals with this type of personality disorder could potentially be vulnerable to cybercrimes such as cyberbullying, harassment, and social engineering due to their peculiar behavior, odd speech (or use of language) and thinking, as well as unusual perceptual experiences [30]. These individuals may feel that they have special powers, like telepathy, or have magical control over others. These symptoms are considered odd by many or eccentric, but they are not psychotic [29]. They may, however, not be as vulnerable to these crimes as some, as even though they exhibit these symptoms, they also find relationships and social interaction difficult and anxiety-inducing. What this means is that they may be less present on social media platforms and have reduced online engagement in social activities, therefore potentially being less likely to be open to these risks. Individuals with this disorder can also be suspicious and paranoid, which may reduce the likeliness of sharing personal information online, opening emails from unfamiliar senders, clicking on links and websites, using dubious USB drives, and more likely to perform proactive cybersecurity activities to protect themselves. However, due to a combination of paranoia, preoccupation with paranormal phenomena, and magical thinking, the internet may provide information such as fake news that will fuel their symptoms.

Antisocial Personality Disorder

This type of disorder is what many would know and refer to as psychopathy or sociopathy [30]. The individual could potentially be a victim of cybercrimes, but it is more likely they will be the perpetrator. This is because deceitfulness and manipulation are central characteristics of the disorder, with poor social conformity and impulsivity. They have little sense of responsibility and can engage in criminal activity, with a lack of

remorse [29]. Individuals with this personality disorder may engage in social engineering as they can utilize their manipulative traits, repeatedly lying, using aliases, and conning others to gain personal profit or pleasure. Individuals with this type of disorder are often aggressive and have violent tendencies that could result in cyberbully, online harassment and cyberstalking [91–93]. These individuals have been reported to engage in rule violations, with criminal activity, such as stealing and pursuing illegal occupations. Therefore, these behaviors can transition to the online world, through hacking, identity theft, creating viruses and ransomware, and even becoming an insider threat to an organization [94]. The individual may have no remorse for others' wishes, rights or feelings, and be indifferent to the harm they have caused. They can also believe that the victim "deserved it", blaming them for being stupid or helpless, and showing little or no empathy for their own criminal actions. With regards to cybersecurity, they may, on the one hand, be more aware of cybercrimes because of their own actions, and undertake proactive cybersecurity behaviors. They could also be less receptive to the trickery of other social engineers, distrusting suspicious emails and not clicking on any links. However, due to the lack of empathy, impulsiveness, extreme irresponsibility, and disregard for their own and others' safety [29], they may adopt risky security behaviors, such as insecure pass- word management practices, and not engage with proactive security practices, such as updating virus software, applications, or patches nor backing up their data, thus increasing their chances of becoming a victim of cybercrimes [57].

Borderline Personality Disorder

Individuals with this type of disorder could potentially be vulnerable to social engineering as through an intense fear of abandonment, they could be vulnerable to criminals manipulating them for their own gain. However, they may enact cyber- crimes themselves, as because of their

intense fear of abandonment [29], they can become inappropriately angry and could express that anger through cyberbullying and harassment. They could also be vulnerable to other cybercrimes such as hacking and identity theft due to their lack of control, and impulsive behavior [61], as they could overshare information, and not engage in cybersecurity behaviors.

Histrionic Personality Disorder

Individuals with histrionic personality disorder exhibit attention-seeking behaviors and are especially concerned with their appearance to gain attention [30]. Owing to their need to be the center of attention, these individuals can be overly trusting, open and flirtatious, which could more easily result in vulnerabilities to cybercrimes, such as, social engineering, especially catfishing, and hacking. In contrast, they too can be manipulative, as well as vain and demanding, and therefore, when they do not receive the attention they require, they can turn aggressive, resulting in online harassment and bullying behaviors. Additionally, individuals with this disorder may believe their relationships to be closer and possibly more profound than they actually are [29], which could also result in online harassment, and cyberstalking. What is more, through their need for social engagement and positive reinforcement from people, when they receive any criticism (particularly with regards to their appearance), this could cause distress. Therefore, with the excessive availability of online complements through selfie posting, the increased probability of criticism is also increased, leading to states of depression and possibly suicidal thoughts and behavior (ibid.). With regards to cybersecurity behavior, individuals with this type of disorder may excessively share personal information and information about those who are around them, due to the individual being more trusting and open [43]. This could result in hacking and identity theft. They may not be overly concerned with protecting themselves and their information, as they have other more pressing concerns of gaining attention and compliments. Therefore, creating strong passwords

may seem an inconvenience when needing to access an online account, and adopting insecure password behaviors such as reusing passwords will seem more appealing. As with password management, updating virus software, patches, and applications, or backing-up information may also not take precedence over their other goals. However, if they are aware of the inconvenience and access issues experienced due to a security incident, they may be more motivated to have good security hygiene to ensure they continue to interact with the online world.

Narcissistic Personality Disorder

Due to being exhibitionistic and the need for admiration, individuals with this disorder could be at risk of social engineering, hacking, ransomware, and cyber- bullying by means of overly sharing information, opinions, and excessive posting. They could also be potentially manipulated by criminals if they believed that information showing them in a less positive light would be revealed. These individuals are often oblivious to the harm they cause to others through their hurtful comments and remarks [29] which could manifest in cyberbullying and harassment online, and could engage with cyberstalking [92, 93]. They, on the flip side, have an extremely fragile self-esteem, which means they are very sensitive to comments and criticism themselves [29]. Therefore, they will excessively lash out in aggression, rage, as well as counterattack and/or become socially withdrawn with a depressive mood. Online interaction with access to positive and negative comments and communication and exacerbate these symptoms. Cybersecurity behavior could be reflected by their awareness of threats—if they are aware of the threats that could undermine their grandiose online persona, they may be more motivated to protect it. Under the belief that they are special and deserve the best [30], they may purchase the “best” antivirus software, and take pride in their proactive cybersecurity behaviors (while believing others are “less” than themselves if they do not take the same proactive stance). With regards to

password security behavior, as with other cybersecurity behavior, it is based on their awareness—if they believe they are creating the "best" password regardless of its strength they will continue to feel secure. However, if they learn that their password behavior is not as secure as they thought, this could lead them to feel unnecessarily inadequate, exacerbating their symptoms.

Avoidant Personality Disorder

Individuals with this type of disorder may be less likely in some ways to be vulnerable to cybercrimes due to the hesitancy in engaging with new activities and social activities. Many individuals with this disorder are anxious about how they are evaluated socially [29]. Although the internet can provide the benefit of anonymous social engagement [77], the disorder could be severe enough that the anonymity would not influence the anxiety levels enough. This also means that if the individual were to engage with online relationships and activities, any negative comments or communication could potentially worsen their condition. These individuals are also less likely to take risks through fear of embarrassment, and they are more likely to appraise "nor mal" situations as potentially dangerous, needing their lives to be more secure [29]. The overestimation of dangerous contexts may result in many being hypervigilant to online risks and cybercrime and lead many to adopt proactive cybersecurity behaviors and be less likely to share personal information [57]. However, as with anxiety disorders, this can go in the other direction. The fear could drive the individual to install many antivirus software programs, contacting the effectiveness of their purpose. Furthermore, their feelings of adequacy may result in them feeling help- less towards protecting themselves online, and adopt avoidance behaviors, ignoring security warnings.

Dependent Personality Disorder

Individuals with this type of personality disorder will be vulnerable to cybercrimes, for example, hacking, online harassment, social engineering.

Through the excessive need for others for emotional support and decision-making, and due to the extreme fear of losing approval this allows the individual to be easily manipulated by criminals. Other online risks are seen by worsening their condition by means of interacting with the online world, as criticism and disapproval support their beliefs of worth- lessness [30]. Individuals with this personality disorder may open suspicious emails and follow the requests within, and use USB drives given to them by criminals in the attempt to being accommodating. Individuals may feel inadequate to protect themselves against any cybersecurity risks of which they are aware. They may additionally depend on others to enact proactive security behaviors and even choose passwords for them. However, their overall feelings and beliefs of inadequacy will drive these individuals to feel helpless in the face of a security threat and influence their motivation to protect themselves.

Obsessive–Compulsive Personality Disorder

Individuals with this personality disorder may be at risk to all cybercrimes, but not necessarily more than individuals without the disorder. Individuals with this disorder are often orderly, have a preoccupation with detail, and have a need to control their environment, affecting their interpersonal and social functioning [30]. They may however, easily find themselves cyberbullying others online if they do not correspond or agree with their rigid thoughts and beliefs. They are followers of rules, procedures and exhibit compliance behavior. These characteristics could result in good cybersecurity practices reducing the chances of becoming a victim of cybercrime. However, if the individual is not fully aware of proper security practices and policies, they may find it difficult to adapt their existing behavior. Furthermore, due to their perfectionism and high standards, to become a victim of cybercrime would potentially have devastating effects on their condition as they are mercilessly self-critical about their own mistakes [29].

5.4.9 Summary of Mental Disorders

In Table 5.3, eight of the 19 classes of mental disorders are summarized together with the benefits and risks of online interaction, and the cyber security behaviors. Each class has a short description of the disorder. The benefits summarize the beneficial themes of internet and digital technology usage and provide examples that are present for each mental disorder class. The risks of online engagement list the present risks for each disorder, and clarify whether the user would likely be the victim and/or the preparator of these risks. The cyber security behaviors refer to whether the user with the specific mental disorder would likely adopt insecure and/or secure behaviors.

Table 5.3. Summary of mental disorders with brief description, online benefits, online risks, and cybersecurity behaviors

Mental Disorder	Brief description	Benefits of online interaction: themes and examples	Risks of online engagement: victim or perpetrator and why	Cyber security behaviors: adoption of secure or insecure behaviors
Neurodevelopmental disorders inc: intellectual disabilities, autism spectrum disorder, ADHD, specific learning disorder	Developmental impairments: vary from specific limitations in learning and in controlling attention to more general impairments in intelligence and social skills.	*Social and communication*: develop and maintain friendships *Cognitive*: develop social skills *Occupational*: education *Independence*: online gaming *Supportive*: health information	*Social engineering*: victim *Online harassment*: victim *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: secure /insecure *Oversharing info*: secure /insecure *Proactive security behaviors*: secure /insecure *Backing-up info*: secure /insecure *Suspicious emails, links, websites, USBs*: secure /insecure
Schizophrenia spectrum and psychotic disorders	Positive symptoms: delusions, hallucinations, disorganized thinking (speech), disorganized or abnormal motor behavior	*Social and communication*: communicate with others *Cognitive*: empress emotions and attitudes *Independence*: online shopping	*Social engineering*: victim /perpetrator *Online harassment*: victim /perpetrator *Identity-related crimes*: victim	*Password management*: insecure *Oversharing info*: insecure *Proactive security behaviors*: insecure *Backing-up info*: insecure

	Negative symptoms: absence of emotions and behaviors	*Supportive*: support groups	*Hacking*: victim *DoS*: victim	*Suspicious emails, links, websites, USBs*: insecure
Bipolar disorders	Manic phase: excitable moods, endless energy, risky behaviors (binge on food, alcohol, drugs, and sex) Depressive phase: hopelessness and guilt, suicidal thoughts, and increased sleep	*Social and communication*: develop and maintain friendships *Cognitive*: emotional expression *Occupational*: work *Independence*: online banking *Supportive*: online therapy and support networks	*Social engineering*: victim *Online harassment*: victim *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: insecure *Oversharing info*: insecure *Proactive security behaviors*: insecure *Backing-up info*: insecure *Suspicious emails, links, websites, USBs*: insecure
Depressive disorders inc: major depressive disorder (MDD)	Feeling of sadness, emptiness, irritable mood. Loss of pleasurable feelings, physical slowness, social withdrawnness, loss of appetite and weight gain	*Cognitive*: emotional expression *Occupational*: work *Independence*: online shopping *Supportive*: support groups. online therapy	*Social engineering*: victim *Online harassment*: victim *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: insecure *Oversharing info*: secure /insecure *Proactive security behaviors*: insecure *Backing-up info*: insecure

				Suspicious emails, links, websites, USBs: insecure
Anxiety disorders inc: generalized anxiety disorder (GAD)	Excessive fear and anxiety. Feelings of worry, panic, paranoia, mind going blank, adopt avoidance behaviors, depression	*Social and communication*: communicate with others, develop and maintain friendships *Cognitive*: emotional expression *Occupational*: work, education *Independence*: online shopping and banking *Supportive*: health information, online therapies	*Social engineering*: victim *Online harassment*: victim *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: insecure *Oversharing info*: secure /insecure *Proactive security behaviors*: insecure *Backing-up info*: insecure *Suspicious emails, links, websites, USBs*: secure /insecure
Obsessive-compulsive disorders	Obsessions and/or compulsions, preoccupation with repetitive thoughts and behaviors. Themes: cleanliness, forbidden thoughts (e.g., sexual, violence, etc.),	*Social and communication*: engaging with society *Cognitive*: expressing emotions and attitudes *Occupational*: work/education	*Social engineering*: victim *Online harassment*: victim *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: secure /insecure *Oversharing info*: secure /insecure *Proactive security behaviors*: secure /insecure *Backing-up info*: secure /insecure

	symmetry, harm and death	*Independence*: online shopping *Supportive*: health information, support groups		*Suspicious emails, links, websites, USBs*: secure /insecure
Neurocognitive disorders: inc: dementia	Cognitive impairments: complex/divided attention, illogical thinking, learning, and recalling, using language, and social cognition	*Social and communication*: communicate with family and friends *Cognitive*: expressing emotions *Independence*: assistive technologies* *Supportive*: for carers* * in more severe cases	*Social engineering*: victim *Online harassment*: victim *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: insecure *Oversharing info*: insecure *Proactive security behaviors*: insecure *Backing-up info*: insecure *Suspicious emails, links, websites, USBs*: insecure
Personality disorders				
Paranoid personality disorder	Pattern of distrust and suspiciousness such that others' motives are interpreted as malevolent	*Social and communication*: develop and maintain friendships, engaging with society *Cognitive*: express attitudes	*Online harassment*: perpetrator	*Password management*: insecure *Oversharing info*: secure *Proactive security behaviors*: secure *Backing-up info*: secure

		Occupational: work /education *Independence*: online banking, shopping *Supportive*: health information, support groups, therapy		*Suspicious emails, links, websites, USBs*: secure
Schizoid personality disorder	Pattern of detachment from social relationships and a restricted range of emotional expression	*Cognitive*: learning *Occupational*: work /education *Independence*: online gaming *Supportive*: health information	*Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: secure *Oversharing info*: secure *Proactive security behaviors*: secure *Backing-up info*: secure *Suspicious emails, links, websites, USBs*: secure
Schizotypal personality disorder	Pattern of acute discomfort in close relationships, cognitive or perceptual distortions, and	*Cognitive*: express emotions and attitudes *Occupational*: work /education *Independence*: online gaming	*Online harassment*: victim *Hacking*: victim *DoS*: victim	*Password management*: secure *Oversharing info*: secure *Proactive security behaviors*: secure *Backing-up info*: secure

	eccentricities of behavior	*Supportive*: health information, support groups, therapy		*Suspicious emails, links, websites, USBs*: secure
Antisocial personality disorder	Pattern of disregard for, and violation of, the rights of others	*Social and communication*: communicate with others *Cognitive*: express attitudes *Independence*: online banking, shopping *Supportive*: health information, support groups	*Social engineering*: victim /perpetrator *Online harassment*: victim /perpetrator *Identity-related crimes*: victim /perpetrator *Hacking*: victim /perpetrator *DoS*: victim /perpetrator	*Password management*: secure /insecure *Oversharing info*: secure /insecure *Proactive security behaviors*: secure /insecure *Backing-up info*: secure /insecure *Suspicious emails, links, websites, USBs*: secure /insecure
Borderline personality disorder	Pattern of instability in interpersonal relationships, self-image, and affects, and marked impulsivity	*Social and communication*: develop and maintain relationships *Cognitive*: express emotions and attitudes *Occupational*: work /education	*Social engineering*: victim *Online harassment*: victim /perpetrator *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: insecure *Oversharing info*: insecure *Proactive security behaviors*: insecure *Backing-up info*: insecure *Suspicious emails, links, websites, USBs*: insecure

		Independence: online banking, shopping *Supportive*: health information, support groups, therapy		
Histrionic personality disorder	Pattern of excessive emotionality and attention seeking	*Social and communication*: develop and maintain friendships, engaging with society *Cognitive*: express emotions and attitudes *Occupational*: work /education *Independence*: online shopping *Supportive*: health information, support groups, therapy	*Social engineering*: victim *Online harassment*: victim /perpetrator *Identity-related crimes*: victim *Hacking*: victim /perpetrator *DoS*: victim	*Password management*: insecure *Oversharing info*: insecure *Proactive security behaviors*: insecure *Backing-up info*: insecure *Suspicious emails, links, websites, USBs*: insecure
Narcissistic personality disorder	Pattern of grandiosity, need for admiration, and lack of empathy	*Social and communication*: develop and maintain friendships, engaging with society	*Social engineering*: victim *Online harassment*: victim /perpetrator	*Password management*: secure /insecure *Oversharing info*: secure /insecure

		Cognitive: express emotions and attitudes *Occupational*: work /education *Independence*: online shopping *Supportive*: health information, support groups, therapy	*Identity-related crimes*: victim *Hacking*: victim /perpetrator *DoS*: victim	*Proactive security behaviors*: secure /insecure *Backing-up info*: secure /insecure *Suspicious emails, links, websites, USBs*: secure /insecure
Avoidant personality disorder	Pattern of social inhibition, feelings of inadequacy, and hypersensitivity to negative evaluation	*Cognitive*: learn *Occupational*: work /education *Independence*: online banking, shopping *Supportive*: health information, support groups, therapy	*Online harassment*: victim *Hacking*: victim *DoS*: victim	*Password management*: secure /insecure *Oversharing info*: secure *Proactive security behaviors*: secure /insecure *Backing-up info*: secure /insecure *Suspicious emails, links, websites, USBs*: secure /insecure
Dependent personality disorder	Pattern of submissive and clinging behavior	*Social and communication*: develop and maintain	*Social engineering*: victim *Online harassment*: victim	*Password management*: insecure *Oversharing info*: insecure

	related to an excessive need to be taken care of	friendships, engaging with society *Cognitive*: express emotions and attitudes *Occupational*: work /education *Supportive*: health information, therapy	*Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Proactive security behaviors*: insecure *Backing-up info*: insecure *Suspicious emails, links, websites, USBs*: insecure
Obsessive-compulsive personality disorder	Pattern of preoccupation with orderliness, perfectionism, and control	*Social and communication*: develop and maintain friendships, engaging with society *Cognitive*: express emotions and attitudes *Occupational*: work /education *Independence*: online banking, shopping *Supportive*: health information, support groups,	*Social engineering*: victim *Online harassment*: victim /perpetrator *Identity-related crimes*: victim *Hacking*: victim *DoS*: victim	*Password management*: secure /insecure *Oversharing info*: secure *Proactive security behaviors*: secure *Backing-up info*: secure *Suspicious emails, links, websites, USBs*: secure

5.5 Conclusion

Out of the 4.3 billion online users [19], around 25% will have mental or neurological disorders [20], and therefore, these disorders need to be considered when reviewing users' cybersecurity behaviors. This chapter has provided an overview of how users' psychopathologies could impact cybersecurity behavior and online interaction from the perspective of different mental disorders. It has brought to light the complexities of how mental disorder characteristics can impact a users' experience while engaging with the online world, including gaining support, being at risk to cybercriminals, and participating in cybercrimes themselves.

An examination of psychopathologies has revealed that of each major class of mental disorder, there are numerous disorders under each category, of which have numerous symptoms. These include social, cognitive, and behavioral impairments, that impede upon the individual's daily functioning and independence. The evidence suggests that whereas engaging with the online world and digital technologies can support the clinical impairments of these disorders through a variety of benefits; users are also at risk of exacerbating their symptoms. Conversely, their symptoms can also in return, exacerbate the risks of becoming victims of cybercrimes, through users' generalized online behavior and their specific cybersecurity behavior. There are several mental disorders whose symptoms, such as disorganized thoughts, lack of judgment, overly trusting, and easily manipulated, could increase a users' likelihood of becoming a victim to various cybercrimes. However, there are many disorders where the symptoms can result in users becoming the perpetrators of cybercrimes. On one hand, several disorders present characteristics that could potentially increase users' cybersecurity, through exhibiting secure/protective behaviors, hypervigilance, and distrust. However, these behaviors, because they are driven by a psychopathology, could in fact have the opposite effect, increasing the chance of becoming a cybercrime

victim.

Previous research has only recently begun to examine psychopathology and abnormal behaviors with respect to interacting with the internet and digital technology (e.g., [8, 20, 28, 36, 66]). With regards to cybersecurity, previous research has studied how cybercrimes affects the psychology of users (e.g., [5]). There have also been several research examining how cognitive attributes affect security compliance and awareness (e.g., [15, 76]) and examining personality traits such as, open- ness, narcissism, impulsiveness, and trust in relation to susceptibility to cybercrimes (e.g., [42, 43, 48, 57]). Nonetheless, there is very little research examining how users' psychopathology affects their interaction online, and next no research examining specific mental disorders and vulnerability to cybercrime [35, 66, 79], and cybersecurity behaviors.

This chapter has begun to address this gap by reviewing a variety of mental disorders and applying their characteristics to the cybersecurity context. Although examining personality traits and cognitive factors can provide some insight into how individuals with mental disorders may perform (or not) cyber secure behaviors, examining specific isolated symptoms does not give an accurate overall representation of how the complexity of these interacting symptoms affects a user's cybersecurity behavior. Furthermore, traits and symptoms when they are "non-clinical" are again, are very different. The criteria of mental disorders are determined by their severity and longevity of symptoms [29]. Therefore, observing the effects of, for example, feeling anxious is very different from observing the effects of the unending, paralyzing pain of worry and paranoia. So too, examining a user who is a "bit particular", is very different from examining a user who experiences the excruciating need to perform an action (even when it is acknowledged as abnormal) because of repetitive intrusive thoughts. However, these symptoms are experienced by a substantial number of users and therefore, need to be considered when

examining users' vulnerability to cybercrimes and the protective actions they perform to secure themselves in the online world.

Acknowledgements I would like to thank Assoc. Professor Rebekah Rousi and Dr. Juuli Lumivalo for all their encouragement and feedback in writing this chapter. I would like to thank Miika Luhtala for his patience, technical expertise and fixing my laptop (a lot) while writing this chapter. I am also grateful to Janne Kohvakka for his constant support.

References

1. Legner C, Eymann T, Hess T, Matt C, Böhmann T, Drews P, Mädche A, Urbach N, Ahlemann F (2017) Digitalization: opportunity and challenge for the business and information systems engineering community. Bus Inf Syst Eng 59(4):301–308
2. Li Y, Dai J, Cui L (2020) The impact of digital technologies on economic and environmental performance in the context of industry 40 a moderated mediation model. Int J Prod Econ 229:107777
3. Nye JS (2011) Nuclear lessons for cyber security? Strateg Stud Q 5(4):18–38
4. Von Solms R, Van Niekerk J (2013) From information security to cyber security. Comput Secur 38:97–102
5. Bada M, Nurse JRC (2020) The social and psychological impact of cyberattacks. In: Benson V, McAlaney J (eds) Emerging cyber threats and cognitive vulnerabilities. Academic Press, pp 73–92
6. Patterson W, Winston-Proctor CE (2019) Behavioral cybersecurity: applications of personality psychology and computer science. CRC Press, Boca Raton, FL
7. Bonneau J, Just M, Matthews G (2010) What's in a name? Evaluating statistical attacks on personal knowledge questions. In: Sion R (ed) Financial cryptography and data security: 14th international conference, FC 2010, revised selected papers. Springer, Berlin, pp 98–113
8. Schneier B (2015) Secrets and lies: digital security in a networked world, 15th edn. Wiley, Indianapolis, IN
9. Herath T, Rao HR (2009) Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst 47(2):154–165

10. Adams A, Sasse MA (1999) Users are not the enemy. Commun ACM 42(12):40–46
11. Anderson R (2020) Security engineering: a guide to building dependable distributed systems, 3rd edn. Wiley, Indianapolis
12. Ponemon Institute (2018) 2018 Cost of a data breach study: global overview. Ponemon Institute LLC
13. Arachchilage NAG, Love S (2014) Security awareness of computer users: a phishing threat avoidance perspective. Comput Hum Behav 38:304–312
14. Grawemeyer B, Johnson H (2011) Using and managing multiple passwords: a week to a view. Interact Comput 23(3):256–267
15. Humaidi N, Balakrishnan V (2015) Leadership styles and information security compliance behavior: the mediator effect of information security awareness. Int J Inf Educ Technol 5(4):311–318
16. Renaud K, Weir GRS (2016) Cybersecurity and the unbearability of uncertainty. In: 2016 cybersecurity and cyberforensics conference (CCC). IEEE, pp 137–143
17. ENISA (2018) Cybersecurity culture guidelines: behavioural aspects of cybersecurity. Euro-pean union agency for network and information security (ENISA). https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjLrLu84aDvAhXto4sKHT0cCW0QFjAAegQIARAD&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications% 2Fcybersecurity-culture-guidelines-behavioural-aspectsofcybersecurity%2Fat_download%2FfullReport&usg=AOvVaw0R_7y4E2KXvtl0iV3jh8iQ
18. Moallem A (ed) (2018) Human-computer interaction and cybersecurity handbook. CRC Press, Boca Raton, FL
19. World Stats (2019) Usage and population statistics. Internet World Stats. http://www.internetworldstats.com/stats.htm. Accessed 1 May 2019
20. WHO (2001) International classification of functioning, disability and health. World Health Organization. https://www.who.int/classifications/icf/en/
21. Whitty MT, Young G (2017) Cyberpsychology: the study of individuals, society and digital technologies. Wiley, Indianapolis, IN
22. Connolly I, Palmer M, Barton H, Kirwan G (eds) (2016) An introduction to cyberpsychology,1st edn. Routledge, New York
23. Carli V, Durkee T, Wasserman D, Hadlaczky G, Despalins R, Kramarz E, Wasserman C, Sarchiapone M, Hoven CW, Brunner R, Kaess M (2013) The association between pathological internet use and comorbid psychopathology: a systematic review. Psychopathology 46(1):1–13

24. Flood C (2016) Abnormal cyberpsychology and cybertherapy. In: Connolly I, Palmer M, Barton H, Kirwan G (eds) An introduction to cyberpsychology, 1st edn. Routledge, New York, pp 153–164
25. Morahan-Martin J (2007) Internet use and abuse and psychological problems. In: Joinson AN, McKenna KYA, Postmes T, Reips U-D (eds) Oxford handbook of internet psychology. Oxford University Press, Oxford
26. Barlow DH, Durand VM (2012) Abnormal psychology: an integrative approach. Wadsworth, Cengage Learning, Belmont, CA
27. Kring AM, Davison GC, Johnson SL, Neale JM (2007) Abnormal psychology. 10th edn. Wiley
28. Norman KL (2017) Cyberpsychology: an introduction to human-computer interaction, 2nd edn. Cambridge University Press, Cambridge
29. APA (2013) Diagnostic and statistical manual of mental disorders (DSM-5®), 5th edn. American Psychiatric Publishing
30. Black DW, Grant JE (2014) DSM-5® guidebook: the essential companion to the diagnostic and statistical manual of mental disorders. American Psychiatric Publishing, London
31. WHO (2019) Mental disorders. World Health Organization. https://www.who.int/news-room/fact-sheets/detail/mental-disorders
32. Bannon S, McGlynn T, McKenzie K, Quayle E (2015) The internet and young people with additional support needs (ASN): risk and safety. Comput Hum Behav 53:495–503
33. Chadwick DD, Wesson C, Fullwood C (2013) Internet access by people with intellectual disabilities: inequalities and opportunities. Future Internet 5(3):376–397
34. Livingstone S, Haddon L (2009) EU kids online. Zeitschrift für Psychologie/J Psychol 217(4):236–239
35. Chadwick DD, Chapman M, Caton S (2019) Digital inclusion for people with an intellectual disability. In: Attrill-Smith A, Fullwood C, Keep M, Kuss DJ (eds) The Oxford handbook of cyberpsychology. Oxford University Press, Oxford, pp 261–284
36. Katz E (1974) Utilization of mass communication by the individual. In: Blumler JG, Katz E (eds) The uses of mass communications: current perspectives on gratifications research. Sage Publications, pp 19–32
37. Ruggiero TE (2000) Uses and gratifications theory in the 21st century. Mass Commun Soc 3(1):3–37
38. Parikh SV, Huniewicz P (2015) E-health: an overview of the uses of the Internet, social media, apps, and websites for mood disorders. Curr Opin Psychiatry 28(1):13–17

39. Wright K (2000) Computer-mediated social support, older adults, and coping. J Commun 50(3):100–118
40. Barak A, Boniel-Nissim M, Suler J (2008) Fostering empowerment in online support groups. Comput Hum Behav 24(5):1867–1883
41. Coulson N, Smedley R (2015) A focus on use of online support. In: Attrill A (ed) Cyberpsychology. Oxford University Press, Oxford, pp 197–213
42. Nurse JRC (2019) Cybercrime and you: how criminals attack and the human factors that they seek to exploit. In: Attrill-Smith A, Fullwood C, Keep M, Kuss DJ (eds) The oxford handbook of cyberpsychology. Oxford University Press, Oxford, pp 663–690
43. Moody GD, Galletta DF, Dunn BK (2017) Which phish get caught? an exploratory study of individuals' susceptibility to phishing. Eur J Inf Syst 26(6):564–584
44. Jones LM, Mitchell KJ, Finkelhor D (2013) Online harassment in context: trends from three youth internet safety surveys (2000, 2005, 2010). Psychol Violence 3(1):53–69
45. Barton H (2016) The dark side of the internet. In: Connolly I, Palmer M, Barton H, Kirwan G (eds) An introduction to cyberpsychology, 1st edn. Routledge, New York, pp 58–70
46. Woods N, Siponen M (2018) Too many passwords? How understanding our memory can increase password memorability. Int J Hum Comput Stud 111:36–48
47. Woods N, Siponen M (2019) Improving password memorability, while not inconveniencing the user. Int J Hum Comput Stud 128:61–71
48. Shropshire J, Warkentin M, Sharma S (2015) Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput Secur 49:177–191
49. Whitman ME (2003) Enemy at the gate: threats to information security. Commun ACM 46(8):91–95
50. Woods N (2019) The light side of passwords: turning motivation from the extrinsic to the intrinsic. In: Proceedings of the 14th Pre-ICIS workshop on information security and privacy at ICIS 2019
51. Campbell J, Ma W, Kleeman D (2011) Impact of restrictive composition policy on user password choices. Behav Inf Technol 30(3):379–388
52. Shay R, Komanduri S, Durity AL, Huh P, Mazurek ML, Segreti SM, Ur B, Bauer L, Christin N, Cranor LF (2016) Designing password policies for strength and usability. ACM Trans Inf Syst Secur 18(4):1–34
53. Das A, Bonneau J, Caesar M, Borisov N, Wang X (2014). The tangled web of password reuse. In: NDSS '14. Internet Society, pp 23–26
54. Hern A (2018) Strava suggests military users 'opt out' of heatmap as row deepens. The

Guardian. https://www.theguardian.com/technology/2018/jan/29/strava-secretarmybase-loc ations-heatmap-public-users-military-ban

55. Furnell SM, Bryant P, Phippen AD (2007) Assessing the security perceptions of personal Internet users. Comput Secur 26(5):410–417
56. Sasse MA, Smith M, Herley C, Lipford H, Vaniea K (2016) Debunking security-usability tradeoff myths. IEEE Secur Priv 14(5):33–39
57. Egelman S, Peer E (2015). Scaling the security wall: developing a security behavior intentions scale (SeBIS). In: CHI'15: proceedings of the 33rd annual ACM conference on human factors in computing systems. pp 2873–288
58. Menard P, Gatlin R, Warkentin M (2014) Threat protection and convenience: antecedents of cloud-based data backup. J Comput Inf Syst 55(1):83–91
59. Crossler RE (2010) Protection motivation theory: understanding determinants to backing up personal data. In: 2010 43rd Hawaii international conference on system sciences. IEEE, pp 1–10
60. Tischer M, Durumeric Z, Foster S, Duan S, Mori A, Bursztein E, Bailey M (2016). Users really do plug in USB drives they find. In: 2016 IEEE symposium on security and privacy (SP). IEEE, pp 306–319
61. Coutlee CG, Politzer CS, Hoyle RH, Huettel SA (2014) An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt impulsiveness scale version 11. Arch Sci Psychol 2(1):1–12
62. Mayes SD, Calhoun SL, Crowell EW (2000) Learning disabilities and ADHD: overlapping spectrum disorders. J Learn Disabil 33(5):417–424
63. Tynes BM (2007) Role taking in online "classrooms": what adolescents are learning about race and ethnicity. Dev Psychol 43(6):1312
64. Chadwick DD, Fullwood C (2018) An online life like any other: identity, self-determination, and social networking among adults with intellectual disabilities. Cyberpsychol Behav Soc Netw 21(1):56–64
65. Chadwick DD, Quinn S, Fullwood C (2016) Perceptions of the risks and benefits of internet access and use by people with intellectual disabilities. Br J Learn Disabil 45(1):21–31
66. Good B, Fang L (2015) Promoting smart and safe internet use among children with neurodevelopmental disorders and their parents. Clin Soc Work J 43(2):179–188
67. Kowalski RM, Fedina C (2011) Cyber bullying in ADHD and asperger syndrome populations. Res Autism Spectrum Disord 5(3):1201–1208
68. GBD 2017 Collaborators (2018) Global, regional, and national incidence, prevalence, and

years lived with disability for 354 diseases and injuries for 195 countries and territories, 1990–2017: a systematic analysis for the global burden of disease study 2017. Lancet 392:1789–1858

69. Becker T, Kilian R (2006) Psychiatric services for people with severe mental illness across western Europe: what can be generalized from current knowledge about differences in provision, costs and outcomes of mental health care? Acta Psychiatr Scand 113(Suppl. 429):9–16
70. McGrath J, Saha S, Chant D, Welham J (2008) Schizophrenia: a concise overview of incidence, prevalence, and mortality. Epidemiol Rev 30(1):67–76
71. Conell J, Bauer R, Glenn T, Alda M, Ardau R, Baune BT, Berk M, Bersudsky Y, Bilderbeck A, Bocchetta A, Bossini L et al (2016) Online information seeking by patients with bipolar disorder: results from an international multisite survey. Int J Bipolar Disord 4(1):1–14
72. Sunderland M, Wong N, Hilvert-Bruce Z, Andrews G (2012) Investigating trajectories of change in psychological distress amongst patients with depression and generalised anxiety disorder treated with internet cognitive behavioural therapy. Behav Res Ther 50(6):374–380
73. Breuer L, Barker C (2015) Online support groups for depression: benefits and barriers. SAGE Open 5(2):1–8
74. Nimrod G (2013) Online depression communities: members' interests and perceived benefits. Health Commun 28(5):425–434
75. Kowalski RM, Giumetti GW, Schroeder AN, Lattanner MR (2014) Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. Psychol Bull 140(4):1073–1137
76. Donalds C, Osei-Bryson KM (2020) Cybersecurity compliance behavior: exploring the influences of individual decision style and other antecedents. Int J Inf Manag 51:102056
77. Erwin BA, Turk CL, Heimberg RG, Fresco DM, Hantula DA (2004) The internet: home to a severe population of individuals with social anxiety disorder? J Anxiety Disord 18(5):629–646 78. Wegmann E, Oberst U, Stodt B, Brand M (2017) Online-specific fear of missing out and Internet-use expectancies contribute to symptoms of Internet-communication disorder. Addict Behav Rep 5:33–42
79. Welk AK, Hong KW, Zielinska OA, Tembe R, Murphy-Hill E, Mayhorn CB (2015) Will the "phisher-men" reel you in? Assessing individual differences in a phishing detection task. Int J Cyber Behav, Psychol Learn 5(4):1–17

80. Woods N (2016) Improving the security of multiple passwords through a greater understanding of the human memory. Dissertation, University of Jyväskylä
81. James TL, Lowry PB, Wallace L, Warkentin M (2017). The effect of belongingness on obsessive-compulsive disorder in the use of online social networks. J Manag Inf Syst 34(2):560–596
82. Holone H (2016) The filter bubble and its effect on online personal health information. Croat Med J 57(3):298–301
83. Astell AJ, Bouranis N, Hoey J, Lindauer A, Mihailidis A, Nugent C, Robillard JM (2019) Technology and dementia: the future is now. Dement Geriatr Cogn Disord 47(3):131–139
84. Clare L, Rowlands JM, Quin R (2008) Collective strength: the impact of developing a shared social identity in early-stage dementia. Dementia 7(1):9–30
85. LaMonica HM, English A, Hickie IB, Ip J, Ireland C, West S, Shaw T, Mowszowski L, Glozier N, Duffy S, Gibson AA, Naismith SL (2017) Examining internet and eHealth practices and preferences: Survey study of Australian older adults with subjective memory complaints, mild cognitive impairment, or dementia. J Med Internet Res 19(10):358
86. Boots LMM, de Vugt ME, van Knippenberg RJM, Kempen GIJM, Verhey FRJ (2014) A systematic review of Internet-based supportive interventions for caregivers of patients with dementia. Int J Geriatr Psychiatry 29(4):331–344
87. Berridge C, Furseth PI, Cuthbertson R, Demello S (2014) Technology-based innovation for independent living: policy and innovation in the United Kingdom, Scandinavia, and the United States. J Aging Soc Policy 26(3):213–228
88. Asbury T, Hall S (2013) Facebook as a mechanism for social support and mental health wellness Psi Chi J Psychol Res 18(3):124–129
89. WHO (2018) Assistive technology. World Health Organization. https://www.who.int/news-room/fact-sheets/detail/assistive-technology
90. Lopresti EF, Mihailidis A, Kirsch N (2004) Assistive technology for cognitive rehabilitation: state of the art. Neuropsychol Rehabil 14(1–2):5–39
91. Bogolyubova O, Panicheva P, Tikhonov R, Ivanov V, Ledovaya Y (2018) Dark personalities on facebook: harmful online behaviors and language. Comput Hum Behav 78:151–159
92. Moor L, Anderson JR (2019) A systematic literature review of the relationship between dark personality traits and antisocial online behaviours. Pers Individ Differ 144:40–55
93. Smoker M, March E (2017) Predicting perpetration of intimate partner cyberstalking:

gender and the dark tetrad. Comput Hum Behav 72:390–396

94. King ZM, Henshel DS, Flora L, Cains MG, Hoffman B, Sample C (2018) Characterizing and measuring maliciousness for cybersecurity risk assessment. Front Psychol 9:39.