

3**Cybercrime and Cyber Psychology:
Understanding Human Behavior,
Psychological Vulnerabilities, and Mental
Health in Digital Era****Priyanka Singh^{1*} & Dr. Fariza Saidin²**¹Phd Scholar, Department of Psychology, Girijananda Chowdhury University, Guwahati, Assam, India.²Assistant Professor, Department of Psychology, Girijananda Chowdhury University, Guwahati, Assam, India.

*Corresponding Author: singhcounsellor@gmail.com

Abstract

Digital technology is changing the way people communicate, connect, get information, manage money, do their jobs, learn, and engage in society. Meanwhile, the digital world has opened the door to new fraud, harassment, exploitation, identity deception, cyberbullying, stalking, manipulation, and other forms of cybercrime. While there are several ways to think about cybercrime, the effectiveness and impact of cybercrime are tied to human psychology. Offences facilitated by the use of technology systems also often involve exploiting vulnerabilities in trust, attention, fear, authority, urgency, social influence, emotional attachment, and decision making. A key framework to consider the human side of digital life is Cyber-psychology. It explores the ways in which the psychological processes of humans and digital technologies interrelate with respect to online identity, communication, relationships, social behavior, digital engagement, and psychological wellbeing. Therefore, social engineering, phishing, online relationship fraud, cyberbullying, cyberstalking, digital relationship abuse, and new varieties of artificial-intelligence deception can be viewed from a technological and psychological viewpoint. Digital engagement can impact interpersonal experiences, but it does not necessarily mean that it is a mental disorder in the case of phubbing, fear of missing out (FoMO), loneliness, and social connectedness. This chapter explores cybercrime from a psychological perspective, as well as social engineering, psychological manipulation, fear and decision making, phubbing and FoMO, isolation and social connectedness, cyber bullying and cyber stalking, digital relationship abuse, cyber victimization, deep fakes problematic digital behavior and the new role of psychologists in cybercrime prevention and psychological intervention.

Keywords: Cyber-psychology, Cybercrime, Manipulation, Phubbing, Fear of Missing Out, Loneliness, Cyberbullying, Cyberstalking, Victimization, Deep Fake, Digital Well-Being, Psychological Intervention.

Introduction

Cybercrime as a Human and Psychological Phenomenon

The internet is no longer just a technology conduit for information transfer. It is now a significant place for people to engage with one another. People connect with family members, form friendships, have close and personal relationships, follow education courses, engage in professional tasks and handle money, obtain health details, buy items, voice their ideas, and create parts of their identities on digital platforms. As technology has become an integral part of everyday life, criminal behavior has also evolved, giving rise to new forms of cybercrime. Cybercrime is any computer-related, digital device, communication technology, digitally stored information-based crime that is illegal. These activities can involve (but are not limited to) financial fraud, phishing, cyberstalking, cyberbullying, online harassment, extortion, dissemination of harmful material, and other technology facilitated offences, as well as identity related offences and unauthorized access. But the psychological aspect of cybercrime requires special attention. There are technical vulnerabilities that cybercriminals can take advantage of, but many of the offences try to exploit vulnerability in humans. A person can be encouraged to give a password, send money, click on a link that looks like it could be a reputable site, give out personal details, or stay in contact with an unknown person because the interaction seems believable, urgent, threatening, emotionally significant, or socially convincing. Think of someone who is getting an email that looks like it is from a bank. There is a message that reads that there is some suspicious activity and that the person's account will be suspended if they don't do immediate verification. A link is provided. The person is concerned that he/she will lose the money and does what they are told. Technological aspect of offense can be fraudulent website or a communication system. The psychological aspect is the perception of threat, urgency, credibility, and responsibility. The difference is at the heart of cyber-psychology. It is not possible to say that the victim is careless or unintelligent. It is possible for cybercriminals to create extremely convincing scenarios that take advantage of common human behaviors. The rational acts are not necessarily to trust somebody who seems to be an authority, to react to an urgent threat, to help somebody who seems emotionally close, or to think about something that seems popular. These would be normal human reactions that can be used as tools for manipulation in misleading environments. Cyber psychology thus advances the conversation from the "Why did the victim click?" To "Why did the victim act the way he or she did?" "What was the offender's psychological situation at the time that made the act seem reasonable, necessary, or 'felt'?" This perspective becomes even more critical as cybersecurity reliant on human interaction. With a very secure technological system, it is possible to be broken when a person agrees to disclose private information or is persuaded to take risky action. The human mind is not a force outside the cyber security system,

then a Human attention, trust, emotion, perception, judgment, and decision making are all factors in digital security. (Dupont & Holt, 2023).

Trust, Authority, Fear, and Psychological Manipulation in Cybercrime

Social engineering is one of the most obvious examples of the psychological aspects of cybercrime. Social engineering is an umbrella term for any effort to manipulate or deceive someone into giving information, access, resources, or act which would otherwise be denied to an offender. The attacker engages not only in technical intrusion but also tries to manipulate the person's behavior. The initial step in the process is usually the establishment of credibility. An offender can pretend to be a bank representative, law enforcement, government official, employer, technical-support specialist, friend, romantic partner, or someone you'd expect to trust. The perpetrator can also search for profiles that are publicly visible or from previous contacts and make the message seem more authentic. After establishing credibility, the accused can then present a request. For instance, an individual can obtain a telephone call from a person claiming to be from a bank employee. The caller tells the person that something strange has happened and requests him or her to confirm account details. The caller might have the caller's name and other basic information. This kind of information can lend an air of legitimacy to bogus communication. Psychologically, it can pass through various phases: recognition, credibility, emotional activation, decision making and compliance. In this process, authority plays a significant role. People often use context clues to determine the validity of information. The attention given to communication that has the appearance of having originated from a reputable institution may thus be greater than the attention given to a message from someone who is anonymous. The psychological importance of fear, authority, and urgency in digital-arrest scams has been explored in recent research specifically (Washo, 2021). One type of fraud can be an offender claiming to be an official or law enforcement, pretending that the person is in trouble with the law. Suppose you receive a video call from someone claiming to be a police officer. The caller states that there is an illegal transaction by you connected to your ID documents. You're told that you must cooperate right now, and if you disconnect the call, then you will suffer serious consequences. Emotions can be fear, uncertainty, confusion, and pressure. The person who did the offense has tried to alter the person's psychological job. The person may go down the "How Can I Solve This Emergency?" path instead of the "Is This Communication Genuine?" path. This is a significant difference. But fear is not always incompatible with rational thinking, and stress does not mean that a person is totally out of control of his or her behavior. Studies within the field of psychology suggest that stress can impact cognition and decision-making, though the impacts can be complex and depend on conditions and individual factors. What is actually meant is that strong emotional arousal, uncertainty, and perceived urgency can shape the way people allocate their attention

and evaluate information. Psychological studies of fear of cybercrime have also been conducted. A systematic review of 28 studies identified a number of factors relating to fear of cybercrime, such as victimization and risk perception, and a relationship between fear and changes or restrictions in behavior. Therefore, fear is capable of having two psychological aspects in the digital environment: it can be as a result of cybercrime or, when deliberately provoked by the offenders, it can also become part of the tool of deception (Brands & Van Doorn, 2022).

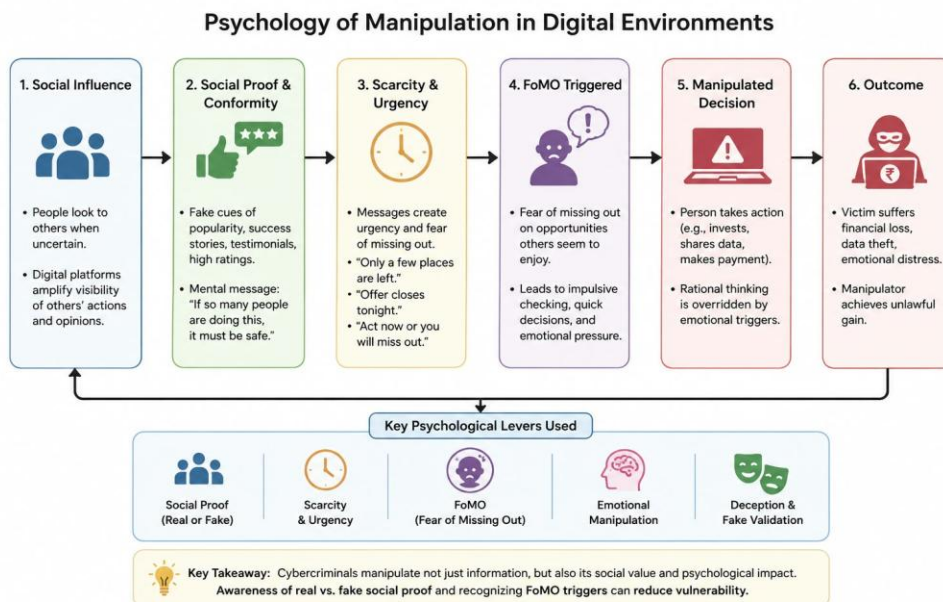
Social Influence, Conformity, FoMO, and Psychology of Manipulation

Social influence is the other psychological factor that is relevant to cybercrime. Human beings are not completely autonomous in the process of decision making. If information is not certain, people can think about what others seem to be doing or thinking. This is a concept that is frequently talked about in the context of social proof and conformity. These processes can be enhanced through the use of digital platforms. For instance, a bogus investment offer might show apparently successful investors, a great deal of people around, good testimony and/or words that the chance is already popular. The person might think that the other's actions are proof that the opportunity is real. The mental message is: ***"If So, Many People Are Doing This, Perhaps It Must Be Safe."*** The offender may then introduce scarcity or urgency: ***"Only A Few Places Are Left."*** ***"The Offer Closes Tonight."*** ***"If You Do Not Act Now, You Will Miss The Opportunity."*** Here comes the fear of losing out; this is where 'FoMO' (fear of missing out) comes into play. The most common definition of FoMO is the fear that others are enjoying fun experiences in life that are not happening to you. In a digital context, FoMO can lead to frequent checking of social-media platforms, messages, notifications, and online activities. The same mental process is also applied in an unethical context. The person may be interested in the financial opportunity, but he or she also feels threatened by the prospect of falling behind as others seem to gain. This doesn't imply that FoMO leads to cybercrime, or that everyone who suffers from FoMO is a victim of cybercrime. Instead, FoMO is a psychological mechanism that could be triggered when intentional strategies are used in digital environments to raise awareness of scarcity, popularity, social exclusion. So it's important to understand the difference between real social proof and fake social proof. A person can get hundreds of positive reviews and think that a product or investment is safe. When these reviews are fake, the social validation psychological cue is created. Thus, cybercrime can also be a manipulation of not only the information but also of its social value. (Ansari et al., 2024)

Emotional Vulnerability, Loneliness, and Digital Relationships

Fundamental human needs for attachment, belonging, recognition, intimacy, and emotional security are also targets of cybercrime. The online dating scam is a good example. An offender can interact with a person via a social media site or

dating website. The offender does not solicit funds at once but comes close overtime. Communication can be regular and intimate. The offender can show concern, affection, sympathy, or commitment. As time passes, the target might start to believe in the relationship. Some time down the road the offender will cause a financial crisis, a health issue, travel problem, or something else that needs help. The manipulation can therefore not start with the financial request can start with building trust and emotional investment. This is very important with regard to loneliness. Loneliness is an individual experience of a lack of enough or satisfaction with social relationships. It's not a synonym for being physically isolated. Being surrounded by others can lead to loneliness, while being surrounded by others can lead to meaningful social connectedness. Digital platforms can offer true connections. They can also be the place where people who are looking for connection come into contact with individuals who are intentionally deceptive themselves. An offender can understand the need for companionship in a person and build a virtual persona to fulfill that emotional want. Vulnerability is not therefore necessarily a weakness on the part of the person (Heinrich & Gullone, 2006). The vulnerability is conceived as the following: the person has a legitimate need to connect with others, and the offender purposefully harnesses these needs. This is also a good illustration of why it is psychologically uncalled for to blame the victim. Victims being fooled by someone who has created a fake identity does not imply a lack of intelligence on the part of the victim. Deception is effective because the deceiver tries to make the false information sound like real information to the victim (Washo, 2021).



Phubbing, FoMO, Loneliness, Social Connectedness and Cognitive Dissonance in Digital Life

- **Cognitive Dissonance**

It is particularly relevant to this contradiction. It is the state of psychological unease which may occur when someone's acts go against their beliefs, attitudes or knowledge. A person may feel that they are using social media too much, impacting sleep, focus, school performance, relationships, and emotional health and wellbeing, but still check the mobile phone regularly. This can then create a feeling of being as if they know that they should cut back on social media, but they feel a sense that they need to check (Festinger, 1957). For instance, a student can make the decision to study for a test and decide to set the phone aside. Once the notification, however, the student reads one message, then accesses a social media app, reads a few posts and then scrolls for a much longer period than anticipated. Later, the student might feel guilty about the behavior because they didn't mean to act that way when they were studying. The following contradiction between intention and behavior is a good example of what cognitive dissonance describes (Festinger, 1957).

- **FoMO**

In the digital world, this conflict can be especially significant by the experience of FoMO. An individual may be aware that frequent social media usage is distracting but may feel concerned about missing out on something important: social contact or event, trend or opportunity, or interaction. This means that it's not as if there aren't competing opportunities for everyone to be more socially active, even though the idea of cutting down on digital interaction is also in the long-term planning phase (Ansari et al., 2024).

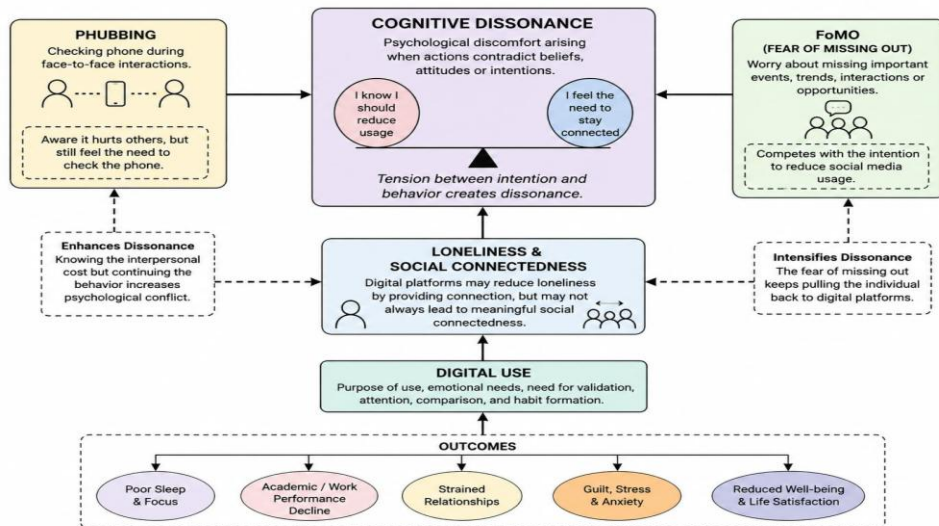
- **Phubbing**

It is another example of this psychological conflict. An individual might be aware that checking a phone several times when talking to someone makes that person feel unimportant, but feel like they need to check the phone or be updated on all the online activity. A person may then be aware of the interpersonal cost of the behavior, yet still persist in the behavior. A systematic review and meta-analysis of 27 studies, including 20,415 participants, showed there was a strong positive relationship between phubbing and FoMO; however, there was significant variation between studies, suggesting that the relationship is not a one-to-one causal process. (Ansari et al., 2024)

- **Loneliness and Social Connectedness**

Loneliness and social connectedness can both further complicate this relationship. Social-media can offer opportunities for communication and belonging, especially if people don't have the luxury of meeting others in person. But frequent

digital contact does not always constitute meaningful social connectedness for an individual. One person can connect with many people online without feeling any closeness to them. This is a significant difference in the psychology between being digitally connected and feeling socially connected. Digital platforms can sometimes help lessen the sense of isolation by providing the opportunity to communicate; however, can it also be a way to seek constant reassurance, attention, or social validation. These processes are significant for cyber psychology because we can't just ask how much time a person spends online to understand digital behavior. The psychological significance of the behavior is determined by how the person uses technology, what emotional or social purpose it serves, if the behavior is coherent with the person's purposes, and if it starts to become problematic in relevant areas of life. The digital space is thus not only a space of technology but also a space of the psychological, in which attention, belonging, social comparison, emotions, and the choices of behavior are constantly interacting.



Cyber Bullying, Cyber Talking and Digital Relationship Abuse

Digital Technology has also, however, altered the manner in which interpersonal aggression, harassment, and relationship-based control may manifest. While the internet can offer a space for communication and socialization, it can also be an arena for intimidation, monitoring, humiliation, threats, or control.

- **Cyberbullying**

It can be harassment, humiliation, threats, social exclusion, impersonation, or the sharing of harmful information through digital channels. Digital content can be persistent and pervasive, which is one aspect of online victimization. For instance, an embarrassing picture posted online could end up being seen by classmates, friends,

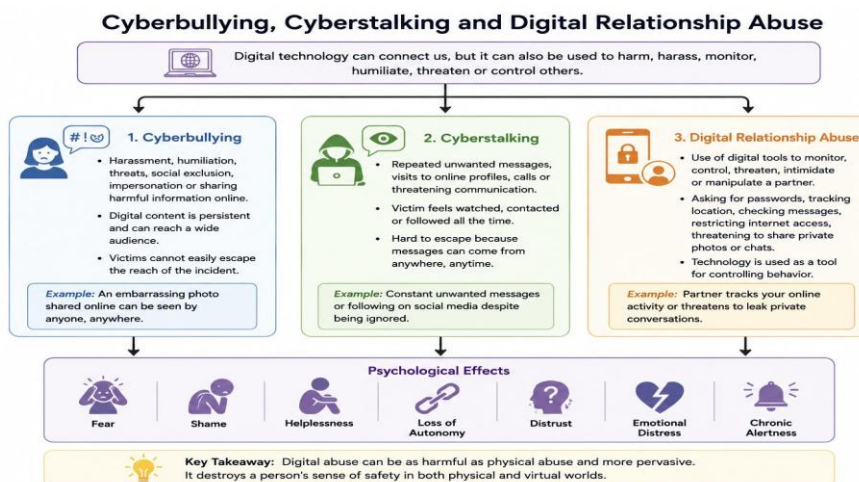
strangers, and other users of a social network. The victim may not be able to clearly define a psychological separation between the environment in which the incident happened and the environment in which he feels safe, unlike many offline incidents (John et al., 2018).

• **Cyber Stalking**

When a person sends unwanted messages, goes to the online site repeatedly, calls or communicates in threatening ways, or otherwise engages in persistent online communication, other people may feel they can't really get away from the person causing the problem. With digital communications being possible from anywhere and at any time, the person could feel like they are being watched, contacted, or followed at all times (Taylor & Xia, 2018).

• **Digital Relationship Abuse**

Abuse that involves the use of digital technology in an intimate or interpersonal relationship to monitor, control, threaten, intimidate or manipulate a partner. A partner might ask for passwords, keep track of social-media contacts, revoke internet privileges, constantly find out where you are, supervise online contacts or threaten to reveal private conversations, photos or other personal information. In these cases, it is not technology that is the cause of the abuse but rather a tool for controlling interpersonal behavior (Taylor & Xia, 2018; Rogers et al., 2023). Psychological effects might be fear, shame, helplessness, loss of autonomy, distrust, emotional discomfort, and chronic alertness. Directing controlling behavior through digital means can also be particularly serious, as it can occur and be more extended than physical abuse and into areas that were deemed to be private. As a result, people can lose their sense of psychological safety in their personal and virtual world. (Rogers et al., 2023).



Problematic Digital Behavior, Cyber Victimization, Psychological Well-Being

This rapid adoption of smartphones, social media, gaming, and other digital mediums have brought opportunities and psychological problems. Digital experience can have a different impact on psychological well-being, depending on how people use digital technologies and whether they have negative experiences online, including cyberbullying, online harassment, fraud, or any other form of online victimization. The psychological impact can be different depending on nature, severity, and duration of experience, age of the person, previous psychological problems, interpersonal skills, social support, and coping resources. When someone loses money due to an online scam, they might feel embarrassed, guilty, angry, or responsible for the loss. A victim of cyberbullying might feel embarrassed, anxious, and insecure, feel isolated from peers, or fear more cyberbullying; constant cyberbullying can also leave a victim feeling insecure. These psychological reactions could persist after the digital incident. For instance, someone who has been fooled might be very suspicious of true communication, and another person might be constantly checking accounts, messages, or devices due to fear of the other incident. The reactions illustrate how cyber victimization can impact psychological functioning in ways other than its digital and material impacts. However, heavy or extended use of technology should not necessarily be viewed as problem behavior. A university student can spend a lot of hours online taking classes, doing homework, chatting with teachers, and doing research. Like that, one person can invest a lot of time in gaming and be academically responsible, be able to go to work, have relationships, sleep, etc. So, it is not possible to determine whether behavior is a problem just by how much time is spent using digital technology. Psychological indicators of digital distress and problematic behavior: psychological assessment considers the type, management, and impact of digital behavior.

Table 1: Digital Stress Indicators

Emotional Distress	Feelings of Fear, Anger, Shame, Humiliation, Helplessness
Anxiety and Insecurity	Ongoing Fear, Repeat Incident, Ongoing Exposure
Self-Blame	Doubt of Judgment, Sense of Responsibility for being Victimized
Social Withdrawal	Avoiding Interactions with others on the Internet after a Negative Experience
Loss Of Control	Digital Dependence that results in craving for the internet.
Functional Impairment	Problems in day-to-day functioning (Relationships, School, Work, Sleep)

Source: Created by Author

This is especially significant when referring to clinical conditions such as gaming disorder, which is now part of the ICD-11. The emphasis is not just on frequency of digital technology, but on a pattern that is related to impaired control

and meaningful disruption of daily functioning. There are significant links between cyber victimization and mental-health issues that have been found through research. There is evidence that links being a victim of cyber bullying and feelings of depression, anxiety, stress, and other psychological distress in youth. This more general psychological rule is to consider digital behavior as a function and its effects, not just whether it occurs or not. The use of digital activities can enhance learning, communication, creativity, employment, social connection, and meaningful recreation. They can, however, become an issue if they are difficult to control, continue after they have become harmful, or get in the way of essential functioning. Cyber-victimization, like in the case of bullying, should also be looked at as part of the individual's wider psychological, interpersonal, social, and contextual situation rather than as a standalone cause of psychological problems. (World Health Organization, 202) (John et al., 2018).

Artificial Intelligence, Deep Fakes, Digital Deception

The rise of synthetic media and their sophisticated production techniques have added a new level of digital deception. With the help of AI, Deepfakes is created or altered versions of media that could make someone appear to say or do something that they never really did. Their value is partly in the psychological value given by man to visual and auditory evidence. As an instance, an employee could obtain a video message that appears to be from a top-level executive, directing him or her to move funds. The face looks familiar, the voice sounds real, and the message is felt as an emergency. The psychological hurdle is right away: (Ching et al., 2025; Diel et al., 2026)

- **Can something that looks and sounds real still be false?**

Deep Fakes can thus introduce challenges to the tasks of trust, credibility evaluation, identification, and factchecking. The harmful uses of deep fakes include fraud, misinformation, impersonation, defamation, and digitally enabled abuse. A scoping review of Deep Fake effects research conducted in 2025 has revealed potential effect areas such as beliefs, memories, behavior, distress, anxiety, self-efficacy, and distrust in media. Meanwhile, the review found little empirical evidence and that the effects of Deep fakes are not yet definitive. This separation is important for proper scientific discussion. As much as Deep fakes are a valid threat to both technology and psychology, there is not enough evidence to confirm that people would simply accept every realistic fake video as true. The psychological reaction is likely to be influenced by a range of factors, including prior beliefs, source credibility, context, familiarity with the represented person, opportunities for independent verification, emotional state, and digital literacy, and Deep fakes present a new need for digital literacy. Evidence of authenticity is no longer just to be seen (Ching et al., 2025; Diel et al., 2026).

- **Psychological Assessment and Intervention**

The psychological reaction to cybercrime needs to start with knowledge of the person's experience. Assessment may include the nature of the cyber incident, emotional reactions, perceived threat, anxiety, depressive symptoms, sleep disturbance, shame, self-blame, interpersonal functioning, social support, and a current sense of safety. Psychologists should also consider whether the digital incident has worsened or worsened the existence of any pre-existing psychological problems (John et al., 2018; Rogers et al., 2023). One may start avoiding social interactions, for instance, due to an encounter with online harassment. A person can end up with a longstanding concern with monetary matters following an internet scam. A person who is suffering from digital relationship abuse might slowly begin to feel uncertain of his or her own instincts. Psychological intervention can thus be more than a discussion of the technological event. Manipulation can be understood and lessens excessive self-blame with psychoeducation. CBT-based strategies can be used to manage ongoing catastrophic thoughts, guilt, or the interpretation of the incident that is irrational. If the individual is still very upset, emotional-regulation and grounding strategies might be helpful. Social support is also crucial. Embarrassment may prevent a victim from reporting an online scam. If a young person is a victim of cyberbullying, he or she may be afraid to speak up for fear of being judged. A person who is a victim of online relationship abuse might think that they will lose the relationship or that others in their family will blame them. Teaching a psychologically safe therapeutic environment enables the person to say what happened without the need for judgmental responses. In cases of high distress and suicidal ideation, timely referral to a mental health professional and appropriate clinical intervention is crucial.

Psychologically Informed Cybercrime Prevention

Cybercrime prevention is often discussed in terms of technical “security” measures such as passwords, authentication systems, software updates, privacy settings, and secure networks. These measures still are vital. But prevention is enhanced when psychological processes are included. People can be taught about suspicious links as well as psychological pressures (John et al., 2018).

For Example:

“Your Account Will Be Blocked Immediately.”

“You Will Be Arrested If You Disconnect.”

“Everyone Has Already Invested.”

“If You Really Trust Me, You Will Help Me.”

“You Must Decide Right Now.”

Statements of this nature should create both psychological and digital caution. They are often created to reduce the time available for a person to pause and think, verify information, consult other one, or consider alternative responses.

From a psychologically informed safety concern, digital interactions that evoke intense fear, a strong sense of urgency, emotional pressure, or unusually heightened excitement should therefore be treated with caution. Every Individual should pause and think after that independently verifies the information before taking any serious action. Although this cannot be considered as a solution of the cyber security protection principle, understanding these emotional cues may help every individual to reduce impulsive compliance with potentially manipulative requests. Cybersecurity education can thus be enhanced by educating people about how manipulation feels, rather than what malicious software looks like (Washo, 2021).

The Emerging Role of Psychologists in Cybercrime Prevention

As technology and human behavior intersect more and more, psychologists have a growing role. There are several ways psychologists can help in cybercrime prevention: by conducting research, delivering psychoeducation, conducting behavioral assessments, counseling, awareness raising, delivering digital well-being interventions, and through interdisciplinary collaboration. The importance of their contribution is especially noteworthy, as cybercrime isn't the same for everyone. Two people can get the same message and react differently. The Information can be checked instantly, or they can reply as a result of the activation of fear, responsibility, trust, or financial concern. These responses can be modified by individual differences with regard to previous experience, digital literacy, emotional state, social support, cognitive processing, and situational pressures. Psychologists can also be involved in designing digital systems and campaigns to minimize human cognitive limitations. A technically correct but psychologically confusing security warning may not work. Likewise, if there is a safety policy that needs to be remembered, consisting of too many complicated procedures, it is likely to be forgotten in a stressful situation. Psychological knowledge can be used to help create interventions that are understandable, realistic, and compatible with human behavior. The psychologist's role is not just to treat the person after they have got hurt. It also covers prevention, education, research, understanding of behavior, fostering resilience, and promoting healthy relationships between people and digital technology.

Future Directions in Cyber Psychology

As Artificial intelligence, synthetic media, immersive environments, algorithmic systems, and more and more personalized digital platforms evolve, the relationship between technology and psychology will grow more and more complex. Future studies should investigate the impact of these technologies on trust, attention, identity, social interaction, emotional regulation, decision making, and psychological well-being. There is also a need for increased focus on the influence of person-environment interaction on digital environments. For instance, for some, FoMO may be more closely associated with digital engagement, and for others, loneliness or a desire for social connection may be more closely related (Dupont & Holt, 2023). The

same social media context could offer valuable connection for one person and lead to such comparisons or distractions for another. An interdisciplinary collaboration between psychology and cybersecurity, criminology and law, artificial intelligence and education, public health, and social sciences is required for the future of cyber psychology. Documented effects, statistical associations, theoretical possibilities, and emerging hypotheses should also be well separated in the research. In fast-evolving fields like artificial intelligence and deepfakes, where public debate debates might outpace hard facts, this scientific prudence is especially vital.

Psychological Prevention, Digital Well-Being and Healthy Digital Habits

The study of cybercrime and the psychological impact wouldn't be complete without looking at how people can be protected and how they can keep themselves psychologically well in today's digitally dominated world. Education, employment, relationships, communication, and everyday decision making are now so well embedded in digital technology that it is not necessarily realistic or desirable to be completely withdrawn from technology. The goal should be to create a healthy, regulated, and psychologically grounded relationship with technology instead. Digital well-being is using digital technologies to enhance, not continually harm, psychological well-being, relationships, productivity, sleep, and daily functioning. This means individuals need to be aware of how much time they spend online, as well as the reasons behind their online use and the psychological need of online behavior. For instance, someone could click on a social media app to view one message only to keep scrolling for a long time. Other people might frequently click on notifications due to FoMO, whereas lonely might be logging on online to get Confirmation or a sense of company. Each scenario has a different psychological meaning of the same digital behavior (World Health Organization, 2020)

- **Digital Detox and Intentional Disconnection**

The one thing that is being talked about more and more is digital detox, which primarily means a conscious decrease in the number of digital gadgets and social media consumed or a short break. digital detox is not about giving up the use of smartphones, social media, or the internet entirely, But it can also mean intentionally setting aside time to avoid focusing on unnecessary electronic activities and to focus on sleep, physical activity, in-person interactions, school or work tasks, hobbies, or other important things. There is some positive evidence for digital detox. Systematic review revealed that digital-detox interventions have significant effects on reductions in depressive symptoms, but not statistically significant effects on life satisfaction, stress, or overall mental well-being (Ansari et al., 2024).

- **Developing Healthy Digital Boundaries**

Establishing healthy online/offline boundaries can assist people establish psychological boundaries. This can sometimes involve technology-free lunchtimes,

designated 'no tech' times for conversation, study or before bed, not having unnecessary alerts and notifications on your devices and making a conscious decision on when and why a technology platform will be used. Setting boundaries is especially important in the context of phubbing. Sustaining interpersonal attention during interpersonal conversation can help to enhance interpersonal presence and inhibit the tendency to split attention between interpersonal conversation and electronic messages. For instance, if two friends are sitting face to face, they can switch their phones off for half an hour while they're discussing something. There's no need to deny the technology; it's about communicating that interpersonal interaction should not be denied. For a student, likewise, it is a choice whether to keep social media apps closed for a designated study time. This establishes an environmental edge, which decreases the necessity to make the same choice in many instances.

- **Managing FoMO and Need for Constant Connectivity**

FoMO can cause people to continually check social media platforms, messages, and notifications as a way to avoid missing out on socially rewarding experiences. Solving FoMO is not just a question of "less screen time. People can become aware of the thoughts that lead to the behavior.

"If I Don't Check Now, I May Miss Something Important"

This thought can be thought about but not followed. Some communications do not have to be responded to in real-time. It's not necessary to mark all social events online. Not all trends are to be followed. Becoming comfortable being disconnected for a while can eventually lead to a healthier relationship with digital information. This is especially relevant as it may make it seem that you have to be available at all times.

- **Strengthening Offline Social Connectedness**

While digital communication can help foster relationships, quality interpersonal relationships also help to foster meaningful social connectedness. Loneliness could be helped if people had a chance to engage in meaningful face-to-face interaction. In community or education, through family engagement, hobbies, peer relationships, and other social engagements. This is especially relevant when online activity is serving as a primary means to meet emotional needs. If a person has a few hours of time to scroll through social media due to loneliness, it may be more beneficial to have them make meaningful interpersonal connections rather than just being told to spend less time on their phone. Therefore, meaningful activities should be used in conjunction with digital reduct.

- **Replacing Passive Digital Consumption with Meaningful Activity**

Digital well-being is not just about the amount of screen time. It also means determining what people do outside the network. Other sources of reward and

psychological engagement can include physical activity, creative activity, reading, hobbies, family interactions, social participation, and adequate sleep. The World Health Organization (WHO) advises children and adolescents to limit sedentary activities, especially those for recreational purposes, and have enough physical activity and sleep. Balanced routines for adults can also help avoid the displacement of sleep, exercise, social interaction, and other activities from the psychological space of digital use each day (World Health Organization, 2020).

- **When Professional Psychological Support is Needed**

Not all digital dysfunctions need to be clinically addressed. But when digital behavior causes distress and/or impairment, a psychological consultation by a professional might be indicated. Persistent anxiety after cyber victimization, extreme social withdrawal, depression, excessive shame, profound sleep disturbance, Compulsive digital behavior, turbulent relationships or thoughts of self-harm are not just issues that can be addressed by telling the person to “use the phone less” and must be assessed psychologically instead. A psychologist will be able to evaluate the person's psychological functioning, look for maintaining factors, reinforce coping mechanisms, work with the person's patterns of thoughts and behaviors, help with emotional regulation, and facilitate the formation of healthier digital and interpersonal patterns. If the psychological distress or risk of self-harm or suicidal behavior is severe, there needs to be a prompt clinical evaluation and appropriate clinical action for safety (John et al., 2018).

- **Towards A Balanced Digital Life**

The Main goal of cyber psychological well-being is not only to create a technology-free society but offer significant benefits for communication, education, healthcare, work, creativity, and social engagement. The Goal is to protect that technology remains a tool that supports human well-being rather than becoming a ruling force that controls attention, influences mood, shapes relationships, or drives decision-making. A well balanced digital life therefore means using technology in a controlled way while maintaining the capacity to manage one's own emotional well-being, relationships, and choices.

Table: Five Principles for a Balanced Digital Life

Awareness	Identification of How and Why Technology is being used
Regulation	Controlling digital actions instead of reacting to each and every notification or online stimulus
Connection	Maintaining Positive Relationships with People Online and in Person
Protection	Understanding Manipulation, Deception, Privacy Issues, and other Cybercrimes
Recovery	Accessing Right Psychological and Social Help when experiencing Digital Evets that cause discomfort

Source: Created by Author

Conclusion

Cybercrime isn't simply a tech issue. It is also a human behavior, perception, emotion, trust, relationship, decision making, and psychological well-being issue. The variety of cybercrime offences shows that the perpetrators can try to exploit common human psychology. Authorities can be employed to establish credibility. Fear can result in a sense of danger. Urgency can generate disincentives for verification. Social influence can establish a perception that an opportunity is good and reliable or popular. There can be an emotional attachment that is used in online relationships. When people worry about missing out on something or a social event, FoMO can come into play. There is a psychological relationship with technology beyond criminal behavior. Smartphone engagement and interpersonal attention are shown to be interfered by phubbing, and research has revealed a high correlation between phubbing and FoMO. Loneliness and the sense of social connectedness also push back the notion that using digital interaction and creating a sense of psychological connectedness are the same thing. Digital relationships and interpersonal aggression and control: cyberbullying, cyberstalking, and digital relationship abuse are examples of how technology can be used as a tool for aggression and control in interpersonal relationships. There has been a link between cyber victimization and psychological problems such as self-harm and suicide attempts among children and young people, highlighting the need to assess and support children's mental health quickly. This is because AI and deep fake technologies further raise the questions of authenticity for visual and auditory information. In the realm of documented and potential applications, deep fakes have been used to commit fraud, misinformation, defamation, and digitally facilitated abuse; however, there exists an emerging body of empirical evidence on the psychological impact of deep fakes (John et al., 2018). The core of cyber psychology is then to have human beings as the focus of digital security. Technology can provide opportunities to connect, learn, create, and work, and participate in society. The same technology can also be used to deceive, exploit, harass, and cause psychological distress. Neither technological pessimism nor technological optimism, but a scientifically based understanding of human behavior in digital environments, is required to perceive this duality. Finally, securing people in the digital world is more than securing devices and networks. It demands learning about the way people think, feel, connect, trust, decide and respond in the digital world. To become more effective at cybercrime prevention, along with technological protection, there will be a need for greater psycho literacy, responsible digital behaviors, evidence-informed intervention, and interdisciplinary collaboration.

References

1. Ansari, S., Azeem, A., Khan, I., & Iqbal, N. (2024). Association of phubbing behavior and fear of missing out: A systematic review and meta-analysis. *Cyberpsychology, Behavior, and Social Networking*, 27(7), 467–481. <https://doi.org/10.1089/cyber.2023.0761>
2. Brands, J., & Van Doorn, J. (2022). The measurement, intensity, and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, 127, 107082. <https://doi.org/10.1016/j.chb.2021.107082>
3. Ching, D., Twomey, J., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G. (2025). Can deepfakes manipulate us? Assessing the evidence via a critical scoping review. *PLOS ONE*, 20(5), e0320124. <https://doi.org/10.1371/journal.pone.0320124>
4. Diel, A., Lalgi, T., Mellis, F. S., Teufel, M., & Bäuerle, A. (2026). The harm of deepfakes: A scoping review of deepfakes' negative effects on human mind and behavior. *AI & Society*, 41, 5971–5987.
5. John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., & Hawton, K. (2018). Self-harm, suicidal behaviors, and cyberbullying in children and young people: Systematic review. *Journal of Medical Internet Research*, 20(4), e129. <https://doi.org/10.2196/jmir.9044>
6. Robert, S. J., Singh, V., Pandey, R. P., & Bhuyan, B. (2026). Digital arrest in the cyber age: A psychological perspective on fear, authority, and consciousness. *Frontiers in Psychology*, 17, 1726740. <https://doi.org/10.3389/fpsyg.2026.1726740>
7. Ansari, S., Iqbal, N., Azeem, A., & Danyal, K. (2024). Improving well-being through digital detoxification among social media users: A systematic review and meta-analysis. *Cyberpsychology, Behavior, and Social Networking*, 27(11), 753–770. <https://doi.org/10.1089/cyber.2023.0742>
8. Ansari, S., Azeem, A., Iqbal, N., & Danyal, K. (2024). Impacts of digital social media detox for mental health: A systematic review and meta-analysis. [Journal details as indexed in PubMed].
9. World Health Organization. (2020). WHO guidelines on physical activity and sedentary behavior.
10. Dupont, b., & Holt, t. J. (2023). Advancing research on the human factor in cybercrime. *Computers in human behavior*, 138, 107410. <https://doi.org/10.1016/j.chb.2022.107410>
11. Festinger, I. (1957). A theory of cognitive dissonance. Stanford University press.

12. Heinrich, I. M., & Gullone, E. (2006). The clinical significance of loneliness: a literature review. *Clinical Psychology Review*, 26(6), 695–718. <https://doi.org/10.1016/j.cpr.2006.04.002>
13. Rogers, M. M., Fisher, C., Ali, p., Allmark, p., & Fontes, I. (2023). Technology-facilitated abuse in intimate relationships: a scoping review. *Trauma, Violence, & Abuse*, 24(4), 2210–2226. <https://doi.org/10.1177/15248380221090218>
14. Taylor, S., & Xia, Y. (2018). Cyberpartner abuse: a systematic review. *Violence and victims*, 33(6), 983–1011. <https://doi.org/10.1891/0886-6708.33.6.983>
15. Washo, A. H. (2021). An interdisciplinary view of social engineering: a call to action for research. *Computers in human behavior reports*, 4, 100126. <https://doi.org/10.1016/j.chbr.2021.100126>.

