THE DIGITAL SECURITY MANUAL

A Roadmap to Online Protection

Maharat
مهارات

THE DIGITAL SECURITY MANUAL
A Roadmap to Online Protection

MODULE

10

Mental Health and Digital Safety
Addressing the psychological impact of digital threats and how to seek help.

Prepared by:
Digital security expert
Bahaa Nasr

The psychological impact of digital threats, such as cyberbullying, stalking, harassment, hacking, and exposure to harmful content can be significant and is often overlooked. Experiencing online attacks in whatever form can seriously jeopardize mental health, self-esteem and overall well-being. It can lead to stress, anxiety, depression, trauma, and even suicidal tendencies especially when people feel their personal safety and privacy have been compromised.

Here's some information to help understand the mental health impact of digital threats and strategies for coping and seeking help.

Which digital security threats can have psychological impact?

Cyberbullying and Online Harassment

Cyberbullying and online harassment are forms of digital abuse that involve using digital technologies to intentionally and repeatedly harm, intimidate, or embarrass others. These behaviors typically occur through various online platforms, including social media, messaging apps, email, and online gaming platforms.

Phishing and Scamming

Phishing and scamming are deceptive practices used by cybercriminals to trick individuals into revealing sensitive information or taking harmful actions. Phishing typically involves fraudulent emails, text messages, or websites that mimic original ones, and try to steal personal data. While scamming includes a broader range of fraudulent activities aimed at financial gain. Both rely on social engineering techniques to manipulate victims.

Data Breaches and Identity Theft

Data Breaches occur when unauthorized individuals access sensitive data, such as personal or financial information, from a company or system. Identity Theft happens when this stolen data is used to impersonate someone, often for fraudulent activities like financial theft.

Ransomware and Cyber Extortion

Ransomware is malicious software that encrypts a victim's data or device, demanding payment for its release. Cyber Extortion involves threats, such as leaking sensitive information, unless a ransom is paid. Both create fear and financial pressure and even physical risk, for example when critical patient files in a hospital are being locked, preventing doctors from providing adequate care.

Stalking and Surveillance (Cyberstalking)

Stalking and Surveillance involve monitoring someone's activities, often online, without their consent to intimidate, control, or harass them. It includes tracking social media, messages, or location data.

Misinformation and Disinformation

Misinformation refers to false information shared unintentionally, while Disinformation is deliberately false content spread to deceive, defame someone, or used in a slander campaigns. Both can distort public perception, fuel fear, and create confusion. They often lead to anxiety and distrust in media, institutions, or public health guidance.

Online Addiction and Overexposure

Online Addiction is excessive, compulsive use of digital platforms, often driven by social media or gaming. Overexposure refers to prolonged screen time, which can disrupt mental health, sleep, and real- connections with other people.

Deepfakes and Manipulated Media

Deepfakes are AI-generated media that create realistic but fake images, videos, or audio, often mimicking real people. Manipulated Media alters content to mislead or deceive viewers. These technologies can erode trust, damage reputations, and cause fear or confusion about what is real.

1. Understanding the Psychological Impact of Digital Threats

Psychological impact of digital threats should be taken seriously, especially in our region where cultural stigma around public shaming can increase the emotional impact. Online harassment, especially gender-based harassment, disproportionately affects women and marginalized groups, leading to increased feelings of isolation, fear, anxiety, depression, and even withdrawal from elections or public life.

Constant Fear, Depression and Anxiety

Digital threats can create a sense of unease and lead to feelings of helplessness, powerlessness, and loss, contributing to depression, anxiety, and even panic attacks. For example, cyberstalking, cyberbullying or harassment can make people feel they are constantly being watched or unsafe, even in their own home. Attacks like these can even lead to suicidal thoughts, and attempts, particularly among adolescents.

Low Self-Esteem and Depression

Hurtful comments, body shaming, or targeted harassment can negatively impact self-esteem and mental health. Especially cyberbullying on social media can lead to a sense of worthlessness, and social isolation. Those targeted might feel judged or unsafe, leading to withdraw from social activities, both online and offline, increasing feelings of loneliness. This is especially dangerous for young people which is why Australia for example decided to ban social media for anyone younger than 16.

Loss of Control and Privacy

You can compare being hacked, impersonated, or doxxed (where personal information is shared publicly without consent) to having someone break into your home. It makes you feel powerless, exposed, violated. When happening online, it creates mistrust in technology, and a constant fear of further attacks. The sudden exposure or loss of privacy often leads to a persistent feeling of vulnerability.

PTSD and Suicidal thinking

Severe cases of online harassment or cyberbullying may even lead to Post-Traumatic Stress Disorder (PTSD) and suicidal thoughts. Victims might feel so overwhelmed by the negativity that they lose hope and consider self-harm as the only way out, particularly among adolescents.

Sleep Disruption

Being exposed to online harassment or data breaches can lead to insomnia and poor sleep quality. Constant stress, fear, and increased alertness will make it impossible to relax which over time contributes to anxiety, depression, and weak cognitive function.
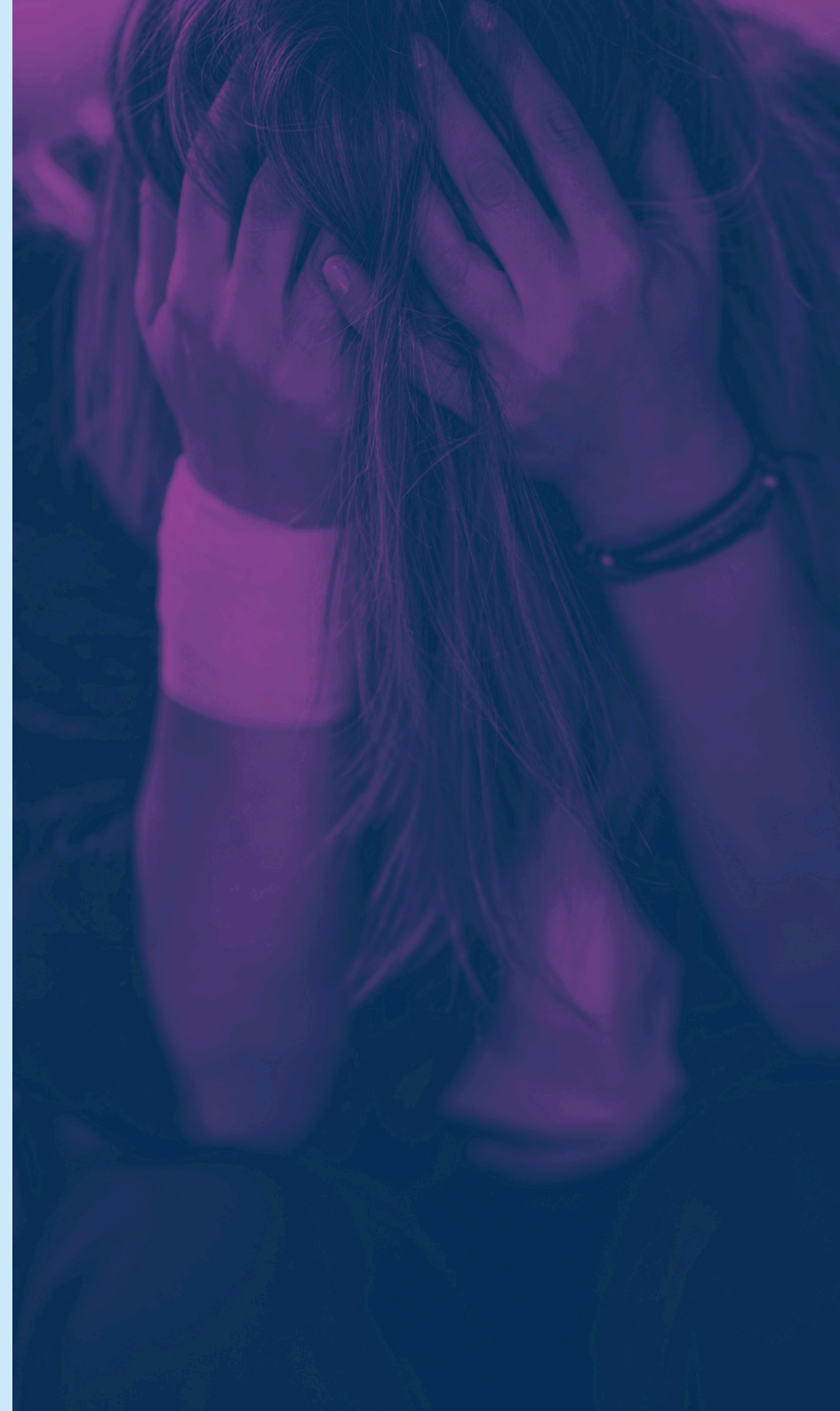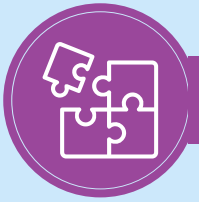
2. Strategies for Coping with the Psychological Impact of Digital Threats

- Consider designating "offline times" to give you mental space to recharge. By limiting the amount of time spent online or on social media you reduce exposure to harmful content.
- Limit Engagement with Harmful Interactions, like avoid responding to online threats or harassment directly, as this can sometimes escalate situations. Use block and report functions to limit and manage negative interactions on social platforms.
- Practice mindfulness and relaxation techniques, meditation, or breathing exercises can help reduce anxiety and stress. These techniques can support you in staying grounded and maintaining emotional stability, especially after a distressing interaction online.
- Focus on positive online spaces, spend time on digital platforms that foster support and positivity. Seek out groups or communities where you feel safe and valued, and avoid platforms that might expose you to negativity or threats.

3. Digital Safety Practices to Reduce Mental Strain

Take Control of Digital Security: Proactively managing your digital security, like using strong passwords, enabling two-factor authentication, and securing your privacy settings, can help you feel more in control and reduce worry over potential threats.

- Strengthen your privacy settings. Limit who can view your content, send you messages, or see your online status.
- Limit the information you share online and set your profiles to private or friends only. Avoid sharing personal information publicly that could be used against you, such as location, daily routines, or identifying details. Consider using aliases where possible to maintain privacy.
- Regularly monitor for personal data leaks, use tools like Google Alerts or services that monitor for personal data leaks, so you get notified if your information appears in unexpected places. Being aware of potential data exposure can help you take swift action if needed before the information spreads widely.
- Prepare steps to take if a digital threat escalates to give you a sense of control. This plan could include identifying who to contact for support, having backup files, knowing how to report issues, and preparing emergency contacts.

4. Seeking Mental Health Support for Digital-Related Anxiety

Acknowledging digital threats and their impacts on mental health is an important first step. Remember: Seeking help is a sign of strength, not weakness. Reach out to friends, family, or support groups who listen and provide guidance. Sharing your experiences with trusted individuals will bring emotional relief and sometimes even practical solutions, and reminds you that you're not alone. Connect with professional therapists who specialize in digital-related anxiety or trauma can help process emotions and develop effective coping strategies.

It's important to take one step at a time. Simple changes, such as limiting screen time or creating a safe digital environment, can significantly improve mental health over time.

It is important to combat stigma related to psycho-social support. Mental health services are confidential, effective and available. Seeking professional help when feeling overwhelmed is vital and should be free of shame.

Seek comfort in community, connect with others who have faced similar digital threats. Engaging and sharing experiences can be therapeutic and help build resilience
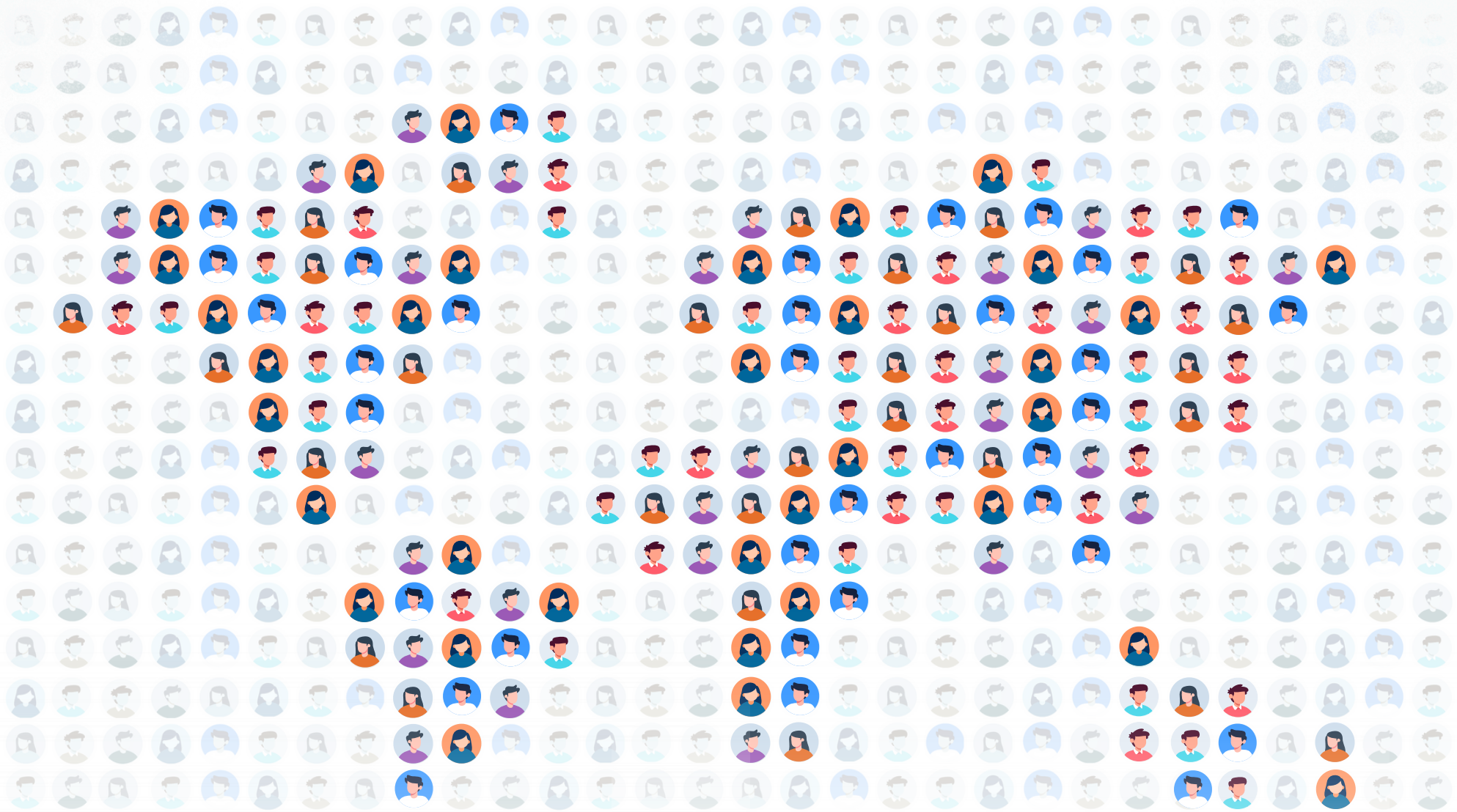
5. Report Digital Threats

Save evidence of all incidents, such as screenshots, emails, and messages to be able to present them when you need.

- **Report Abuse and Harassment to Platforms:** Social media sites, email providers, and messaging apps usually offer reporting mechanism to address abusive behavior. Reporting can lead to account suspension for the offender and reduces your exposure to further threats. It is important to make the reporting from the account of the victim, and reports from friends would support the original report.

- **Notify Law Enforcement for Serious Threats:** If threats escalate to a level where personal safety is at risk, such as physical threats or stalking, it's important to involve law enforcement.

- **Learn about Cyberstalking Laws** and resources available in your country. Most countries nowadays have laws that cover cyberstalking, harassment, and online threats. Check with legal resources or online safety organizations to understand your legal rights and options.

- **Consider reaching out:** to digital rights and advocacy organizations in your country and region. They might have experience with similar cases, and be able to provide resources and support, especially in navigating privacy laws and rights.

Remember, help is always available, and seeking it is a powerful step toward reclaiming control and peace of mind. By taking the right steps you can create a stronger foundation for managing digital threats and their psychological effects. And by seeking appropriate support, you can work toward fast recovery, better resilience and security, also peace of mind.