

QUESTIONNAIRE: PSYCHOLOGICAL CORRELATES OF CYBER BEHAVIOUR AND CYBERCRIME VICTIMISATION

For university students in Delhi NCR

Important source note: The manuscript describes the questionnaire structure, constructs, item counts, and examples of content, but it does not reproduce the verbatim questionnaire items. Therefore, this PDF is a **reconstructed questionnaire aligned with the manuscript**. It should be submitted as the exact survey instrument only if these statements match the questionnaire that was actually administered.

Questionnaire structure stated in the manuscript: Cybercrime Awareness (CCA) - 15 items; Online Privacy Concern (OPC) - 12 items; Cyber Secure Behaviour (CSB) - 10 items; Cyber Insecure Behaviour (CIB) - 10 items; Cybercrime Victimization (CCV) - 10 items. Total: 57 items.

Participant instructions: Please read each statement carefully and select the response that best represents your view or experience. Do not write your name or any personally identifying information on this form.

Section A - Cybercrime Awareness (CCA) - 15 items

This section reflects knowledge and awareness of cyber threats such as phishing, online fraud, data breaches, privacy and digital safety.

Response scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Statement	1	2	3	4	5
1	I can recognize common signs of phishing emails, messages, or websites.					
2	I understand the warning signs of online fraud and digital scams.					
3	I know that data breaches can expose personal and confidential information.					
4	I understand that weak or reused passwords increase the risk of cybercrime.					
5	I know that suspicious links and attachments may contain malware or harmful software.					
6	I understand that sharing personal details online can increase the risk of identity theft.					
7	I know that using unsecured or public Wi-Fi can create security risks.					
8	I know that two-factor authentication can improve account security.					
9	I understand how privacy settings can reduce unnecessary exposure of personal information.					
10	I know that regular software and device updates can reduce security vulnerabilities.					
11	I know that cyberbullying and online harassment can be reported through appropriate channels.					
12	I know how to check whether a website, application, or online source is authentic before using it.					
13	I know how and where to report suspicious or fraudulent online activity.					
14	I understand the risks associated with oversharing personal information on social media.					
15	I understand that cybercrime can affect financial security as well as psychological wellbeing.					

Section B - Online Privacy Concern (OPC) - 12 items

This section reflects concern about personal data protection, privacy, tracking, data sharing and unauthorized access.

Response scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Statement	1	2	3	4	5
1	I am concerned that websites or applications may collect my personal information without my full knowledge.					
2	I am concerned that my personal data may be shared with third parties without my permission.					
3	I am concerned about sharing my location, photographs, contact details, or other personal information online.					
4	I worry that someone may gain unauthorized access to my online accounts.					
5	I am concerned about how long online services store my personal data.					
6	I pay attention to privacy policies or privacy notices when using digital services.					
7	I am concerned about the permissions requested by mobile applications.					

No.	Statement	1	2	3	4	5
8	I am concerned that my online activities may be tracked for purposes I do not fully understand.					
9	I worry that a data breach could expose my personal information.					
10	I am concerned about the privacy and security of online financial transactions.					
11	I worry that my personal information could be misused for impersonation or identity theft.					
12	I prefer to have control over what personal information is collected, stored, and shared about me online.					

Section C - Cyber Secure Behaviour (CSB) - 10 items

This section reflects safe online practices such as password protection, privacy settings and verification of digital content.

Response scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Statement	1	2	3	4	5
1	I use strong and unique passwords for important online accounts.					
2	I change a password when I believe an account may have been compromised.					
3	I use two-factor authentication or another additional security step whenever it is available.					
4	I review and use privacy settings on social media and other online accounts.					
5	I check links, email addresses, or website details before opening suspicious content.					
6	I keep my phone, computer, applications, and security software updated.					
7	I use security tools such as antivirus, device protection, or safe-browsing features where appropriate.					
8	I avoid carrying out sensitive activities, such as banking, on unsecured public Wi-Fi.					
9	I log out of accounts on shared or public devices.					
10	I review application permissions and restrict unnecessary access to my personal information.					

Section D - Cyber Insecure Behaviour (CIB) - 10 items

This section reflects risky online practices such as oversharing, using unverified links or sources, and weak security habits.

Response scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

No.	Statement	1	2	3	4	5
1	I use the same password for more than one online account.					
2	I sometimes click links or attachments from unknown or unverified sources.					
3	I share personal information publicly on social media or other online platforms.					
4	I accept friend, follow, or connection requests from people I do not know personally.					
5	I download files, applications, or software from unverified sources.					
6	I delay or ignore important software and security updates.					
7	I use public or unsecured Wi-Fi for activities involving sensitive personal information.					
8	I have shared or would share confidential security information, such as an OTP or password, when asked online.					
9	I sometimes leave my online accounts logged in on shared or accessible devices.					
10	I interact with unverified online messages, offers, links, or accounts without first checking their authenticity.					

Section E - Cybercrime Victimization (CCV) - 10 items

This section reflects experiences of cyber incidents including fraud, hacking, malware, privacy violations and online harassment.

Response scale: 1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Very Often.

No.	Statement	1	2	3	4	5
1	I have received a phishing email, message, or link intended to obtain my personal information.					

No.	Statement	1	2	3	4	5
2	I have experienced an online fraud or scam attempt.					
3	One of my online accounts has been hacked or taken over without my permission.					
4	My personal information has been misused for impersonation or identity-related purposes.					
5	My device or account has been affected by malware or other harmful software.					
6	I have experienced unauthorized access to an online account or digital service.					
7	I have experienced online harassment, threatening messages, or abusive digital communication.					
8	Someone has created or used a false profile/account to impersonate or misrepresent me.					
9	I have experienced financial loss or an unauthorized transaction connected with an online incident.					
10	I have experienced exposure, leakage, or misuse of personal data that affected my privacy.					

Scoring note: Higher section scores indicate higher levels of the construct being measured. For CCV, a higher score indicates more frequent cybercrime victimisation experiences. The manuscript reports analysis using SPSS and AMOS with descriptive statistics, reliability analysis, Pearson correlation, multiple regression and Structural Equation Modelling (SEM).