



JAGORON

Digital guide: cyber safety and digital responsibility

STOP

Don't react immediately.

CHECK

Is this message, link, software, account or request trustworthy?

SECURE

Fix your device, account and privacy settings.

SWITCH

Choose safer behaviour and legitimate or open-source alternatives.

Project Jagoron, World University of Bangladesh

Updated October 2026

Latest version: <https://cyberjagoron.org/>



SDG initiative by
WORLD UNIVERSITY
OF BANGLADESH
Department of Computer Science and Engineering



Contents

Check your digital privacy	3
Secure your device	4
Crack, risk, switch	5
Before you click	6
Cyberbullying: check, save, report	7
Where to report	9
What would you do?	10
About Jagoron and SDG 16	14
Download and share	15



Booth 1

Check your digital privacy

What does the internet know about you? Open your own settings and mark each line. Nothing you tick leaves your phone.

My Facebook or Instagram profile is not public to strangers	☐ Good	☐ Fix
Only people I choose can see my phone number	☐ Good	☐ Fix
Only people I choose can see my email	☐ Good	☐ Fix
Strangers cannot send me messages	☐ Good	☐ Fix
My friend list is not public	☐ Good	☐ Fix
Not everyone can tag me	☐ Good	☐ Fix
Location sharing is off unless an app really needs it	☐ Good	☐ Fix
I know which apps can use my location	☐ Good	☐ Fix
I know which apps can use my camera and microphone	☐ Good	☐ Fix
I only share what I'd put on a university notice board	☐ Good	☐ Fix

Your score: mark each line to see it

0 to 2 Fix: Good

3 to 5: Needs attention

6 or more: High risk

Quick fixes

Facebook

Settings and privacy, then Privacy Checkup. Set profile details, posts and friend list to Friends or Only me.

Instagram

Settings and activity, then Account privacy, then turn on Private account.

WhatsApp

Settings, then Privacy. Set Last seen, Profile photo and About to My contacts.

Android

Settings, then Privacy, then Permission manager. Review Location, Camera and Microphone.

iPhone

Settings, then Privacy and Security. Review Location Services, Camera and Microphone.

Location rule

Choose "While using the app" for apps that need it, and "Don't allow" for the rest.

Menu names change with app updates and phone brands. Use the search bar in Settings.

If you wouldn't put it on a university notice board, think twice before putting it online.



Booth 2

Secure your device

If you lost your phone right now, could someone open it? Ten minutes is enough to:

Message your contacts

"Brother, I'm in an emergency. Please send BDT 5,000 to this number."

Open your email

and reset your other accounts

See your private photos

a serious privacy violation

Open payment apps

and try unauthorised transactions

Change your settings

and lock you out

Post as you

and damage your reputation

The attacker doesn't need hacking tools. Sometimes the weakness is simply an unlocked phone.

Fix it now

Do the first three now. Finish the rest at home.

- ☐ PIN or password is on
- ☐ Fingerprint or face unlock is on
- ☐ Auto-lock is set to 30 seconds or 1 minute
- ☐ Phone software is updated
- ☐ Apps are updated
- ☐ Find My Device (Android) or Find My (iPhone) is on
- ☐ WhatsApp two-step verification is on
- ☐ 2FA is on for email, Facebook and my university account
- ☐ Lock-screen notifications hide private content

0 of 9 done



Booth 3

Crack, risk, switch

Why do people use cracked software? It's free, it's easy, everyone does it. Here is what you can't see.

Cracked software



Unknown modification



Possible malware or unwanted software



Credential and session theft



Data loss and privacy loss



Account compromise

You don't know what was modified, what you're installing, or what it is doing.

Switch to software you can trust

You need	Try	Type	Official site
Documents	LibreOffice	FOSS	libreoffice.org
Photo editing	GIMP	FOSS	gimp.org
Vector graphics	Inkscape	FOSS	inkscape.org
3D and animation	Blender	FOSS	blender.org
Video editing	Kdenlive	FOSS	kdenlive.org
Video editing	DaVinci Resolve (free version)	Free	blackmagicdesign.com

- Download only from the official site.
- FOSS means free and open source. Free is not always open source.
- Ask your university about student licences before you reach for a crack.

Don't only ask: Is it free? Ask: Can I trust what I'm installing?



Think first

Before you click

Four steps for any message, link or request that feels urgent.

STOP

Don't react. Scammers want you in a hurry.

CHECK

Sender, link, urgency, and any request for money or a password.

VERIFY

Call or meet the person another way. Never use the link in the message.

ACT

Report it, block it, then delete it.

Messages like these are scams

"Urgent! I need BDT 3,000. Send it now."

"Your university account will be disabled today. Click here immediately."

"You won a prize! Share your details to claim it."

Call, don't reply. If a friend asks for money, confirm by phone call first.



Be an upstander

Cyberbullying: check, save, report

Is this cyberbullying? If any of these is true, it is worth acting on.

- ☐ Someone keeps sending me insulting or threatening messages
- ☐ A group is leaving me out or making fun of me online
- ☐ My photo or video is shared or edited without my permission
- ☐ A fake account is using my name or photo
- ☐ Someone is threatening to leak private things unless I pay or obey
- ☐ My private chat or photos were shared publicly
- ☐ I'm being tagged or posted about to humiliate me
- ☐ Someone follows me across apps and won't stop
- ☐ I feel afraid, ashamed or anxious to open my phone

It is not your fault. The person bullying is responsible, and you do not have to handle it alone.

If it happens to you

STOP

Don't reply, don't pay, don't meet. Don't delete anything yet.

SAVE

Screenshot with the date, username and link. Save the chat and profile URL. Note the times.

SECURE

Block the account, change passwords, turn on 2FA, make your profile private, log out of other devices.

REPORT

Platform, then campus, then police or a helpline (next section). Tell someone you trust.

If you see it happen to someone else

- Don't share it, don't comment, don't laugh.
- Save evidence and support them privately.
- Report the post or account, and help them use the routes below.



Get help

Where to report

On campus

Class teacher / Department head	Contact your department
Proctor / Student affairs / Disciplinary committee	Phone: 09643204060, Ext-102
Sexual and gender-based harassment complaint committee	Contact the university complaint committee
Counselling cell or trusted teacher	Contact the counselling cell or a trusted teacher
IT cell / Jagoron cyber team (hacked accounts, technical help)	Contact the university IT cell

Outside campus (Bangladesh)

999	Immediate danger National emergency number
109	Women and children facing violence, including online National Helpline, Department of Women Affairs (reported as 24/7)
1098	Child in danger or being bullied (under 18) Child Helpline
01320000888	Police Cyber Support for Women (PCSW) Also: Facebook page "Police Cyber Support for Women" and cybersupport.women@police.gov.bd
01320010146	CID Cyber Police Center Hotlines 01320010146, 01320010147 and 01320010148
GD	Any serious threat Go to your local police station and file a General Diary (GD) with your evidence.
App	Fake profile or abusive content Use the in-app Report on Facebook, Instagram, WhatsApp, TikTok or YouTube.
Photos	Intimate photos shared or threatened Adults: stopncii.org . Under 18: takeitdown.ncmec.org .

Online harassment, blackmail and sharing intimate images without consent can be crimes in Bangladesh under its cyber-security law. This guide is not legal advice. Civil society groups such as Bangladesh Mahila Parishad, ActionAid Bangladesh, Digitally Right and PrivaC also support people facing online abuse.



Practise

What would you do?

Ten real situations. Tap an answer to see the best choice. Nothing is recorded.

Privacy

Card 1

A stranger sends you a friend request. You share 3 mutual friends.

- A** Accept: you have mutual friends
- B** Accept, then look at their profile
- C** Check their profile and ask a mutual friend first
- D** Accept and send them your number

Best answer: C. Check their profile and ask a mutual friend first

Why. Fake accounts add real friends to look genuine. Check how old the profile is and what it posts, and ask first.

Watch out. B feels safe, but by then they can already see your posts.

Privacy

Card 2

A photo-editing app asks for your camera, contacts and location.

- A** Allow everything so it works
- B** Allow only what editing needs
- C** Allow all now, check later
- D** Use it without reading anything

Best answer: B. Allow only what editing needs

Why. An app should get only what it needs to do its job. A photo editor does not need your contacts or location.

Watch out. C: "later" rarely comes.

A friend posts a photo of you that you don't like.

- A** Post an embarrassing photo of them
- B** Ask them to remove it; untag or report if they refuse
- C** Say nothing and hope it goes away
- D** Comment angrily under the post

Best answer: B. Ask them to remove it; untag or report if they refuse

Why. Start with a calm request. You can untag yourself and report the post if it is not removed.

Watch out. D: anger in public makes it spread.

Your phone has said "Update available" for 3 weeks.

- A** Ignore it; the phone works fine
- B** Update it: updates fix known security holes
- C** Wait for the next version
- D** Turn off update notifications

Best answer: B. Update it: updates fix known security holes

Why. Attackers use known holes in old versions. Updating closes them.

Watch out. A: "works fine" means you can't see the problem.

You lose your phone and it has no screen lock.

- A** Hope an honest person finds it
- B** Lock it with Find My Device, change passwords from another device
- C** Wait a few days before doing anything
- D** Only block the SIM

Best answer: B. Lock it with Find My Device, change passwords from another device

Why. Lock or erase it remotely, then change your email and social passwords. Add a screen lock to your next phone.

Watch out. D: blocking the SIM does not protect your apps and accounts.

A friend's WhatsApp says: "Urgent! I need BDT 3,000. Send it now."

- A** Send it immediately
- B** Reply on WhatsApp and ask why
- C** Call your friend another way to confirm
- D** Forward it to see if others know

Best answer: C. Call your friend another way to confirm

Why. Their account may be hacked, and a reply goes to the attacker. A call confirms who it really is.

Watch out. B: replying keeps you talking to the attacker.

A friend gives you a "pre-activated" version of expensive software.

- A** Install it immediately
- B** Turn off antivirus first
- C** Look for a legitimate or free alternative
- D** Ask someone to send another crack

Best answer: C. Look for a legitimate or free alternative

Why. You can't know what was changed inside it. A free or student version is safer.

Watch out. B: switching off protection is often the first step of an attack.

A download site tells you to disable your antivirus before installing.

- A** Disable it and continue
- B** Stop. That is a red flag
- C** Disable it for five minutes only
- D** Ask a friend to install it for you

Best answer: B. Stop. That is a red flag

Why. Legitimate software never needs your protection switched off.

Watch out. C: five minutes is enough for malware to settle in.

An edited photo of a classmate is going around a group chat.

- A** Share it; it's funny
- B** Don't share; save evidence, support them and report
- C** Ignore it; it's not your problem
- D** Comment "haha" so you don't look soft

Best answer: B. Don't share; save evidence, support them and report

Why. Sharing makes you part of it. Saving evidence and supporting them helps, and reporting can stop it.

Watch out. D: a laugh still spreads it and hurts them.

A fake account is using your friend's name and photo.

- A** Ignore it
- B** Follow it to see what happens
- C** Tell your friend, report the account and use the report routes
- D** Message the fake account to threaten them

Best answer: C. Tell your friend, report the account and use the report routes

Why. Your friend needs to know. Reports from several people can speed up removal.

Watch out. D: threatening back can make things worse and put you at risk.



Why it matters

About Jagoron and SDG 16

Jagoron means awakening. A safe campus online is a peaceful and just campus: students know their rights, protect their privacy, and know where to report.



Peace, Justice and Strong Institutions. Jagoron supports targets on reducing violence and harassment (16.1), protecting children from abuse and exploitation (16.2), access to justice (16.3), accountable institutions (16.6), inclusive and participatory decisions (16.7), and access to information and protection of fundamental freedoms (16.10).

Project Jagoron, World University of Bangladesh.



Take it with you

Download and share

The PDF has the same content as this page, for offline reading and printing. Link: <https://cyberjagoron.org/>

