CYBER CRIME TOOLKIT

UNMASK'D

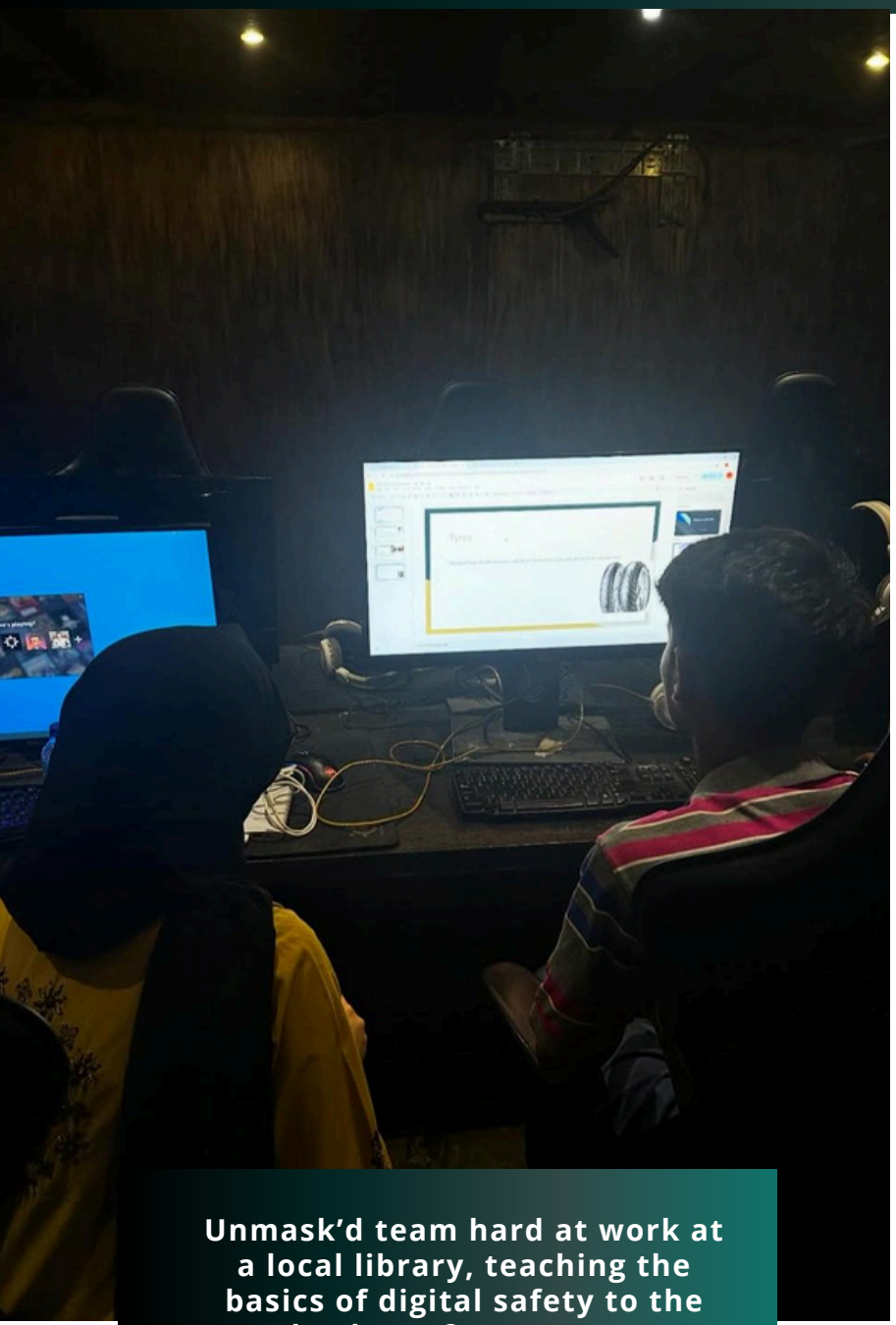
EMPOWERING DIGITAL CITIZENS

A PRACTICAL GUIDE TO ONLINE SAFETY, CYBER HYGIENE, AND LEGAL AWARENESS IN PAKISTAN

TEACHER'S HANDBOOK

WWW.UNMASKD.ORG

CONTENTS



Unmask'd team hard at work at a local library, teaching the basics of digital safety to the leaders of tomorrow.

Author's Note

When I first started Unmask'd, I never imagined it would grow into something this big - that it would actually be taught in schools across Karachi. What started as my little idea to help young women navigate online spaces safely has turned into a toolkit that I hope empowers students to think critically about their digital lives. Seeing it reach classrooms has honestly been surreal.

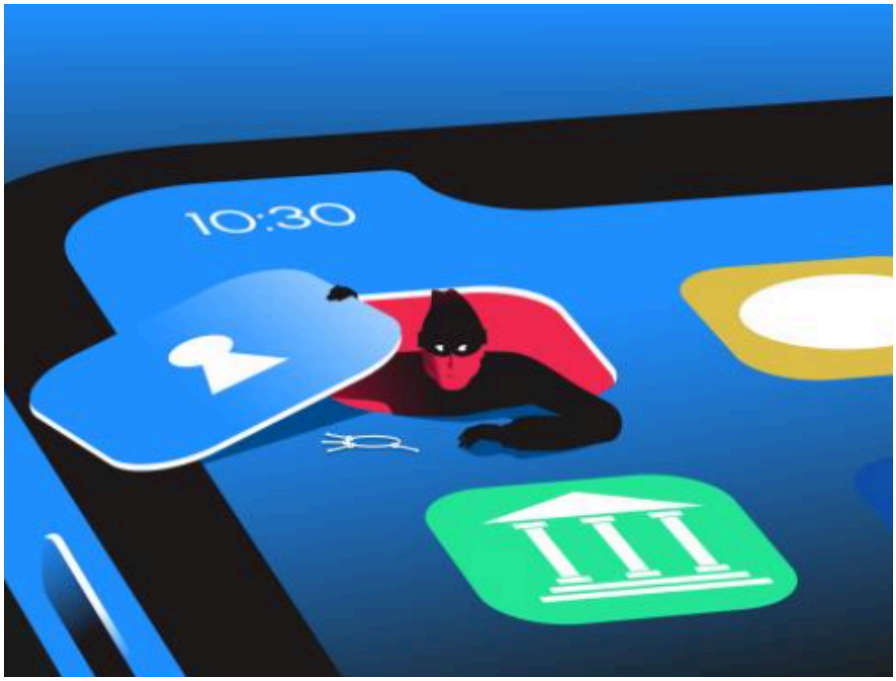
I never imagined my idea could grow this big, and I hope Unmask'd continues to spark conversations, empower young women, and help students take control of their online lives with confidence. Most of all, I hope it helps you the way it helped me, teaching me lessons, giving me perspective, and showing me how much small actions can matter.

Of course, how could I forget my amazing team. A huge thank you to Aahil and Amnah for the countless sleepless nights you spent listening to my rants, giving feedback, and helping me figure out how to turn my chaotic ideas into something practical. To Haania, thank you for making the activities and lessons actually fun and engaging, without you, this would have been a lot less lively. And to the rest of you who worked behind the scenes, helping me propagate it in schools, sending emails, talking about it at seminars, and supporting in every little way, I am so, so thankful. Every small bit of advice, late-night brainstorm, and encouragement made Unmask'd what it is today.

Zehrah Minal
Founder and CEO at Unmask'd

Understanding Cybercrime

Spot the Red Flag: Present students with 4–6 example messages, posts, or friend requests. Ask them to identify which ones might be risky and why. Discuss as a class. Include examples affecting both boys and girls.



THE DEFINITION

Cybercrime is any illegal or harmful activity that happens using computers, smartphones, or the internet. It's not just hackers in movies - it's very real, and it can happen to anyone. From stolen passwords to fake social media accounts, from phishing scams to harassment online, the digital world has risks that are easy to overlook if you're not careful. But here's the thing: cybercrime isn't always about technology. In Pakistan, it often mixes with social and cultural realities. For many young women, a leaked image, a threatening message, or a hacked account can carry consequences far beyond money or data. It can affect your safety, reputation, and even freedom. When online harm interacts with offline expectations of honor and modesty, the stakes rise dramatically. Even if you're confident using social media or apps, small mistakes can lead to big problems. A fake friend request, a suspicious link, or sharing personal info without thinking can put your accounts - and sometimes your personal life - at risk. But everyone, men or women, can face scams, identity theft, or bullying online, so awareness is crucial for all.

HOW UNMASK'D HELPS:

- Phishing Detector & Password Checker: Simple, icon-based tools that show when something is suspicious.
- Legal Aid Chatbot: Explains what is a cybercrime and what you can do, in easy Urdu/English.
- Safety Quiz & Impact Tracker: Interactive games to test knowledge and track your safety.
- Case of the Month Blog: Real-life stories to learn from others' experiences safely.

Have you ever received a message or link online that made you uncomfortable? How did you respond? What could you do differently if you knew more about cybercrime?

QUICK TIPS

- Never share your password, even with friends or family.
- Check links and messages carefully before clicking.
- Think before sharing personal information or photos.
- If something feels wrong, report it to a trusted adult or teacher.

TYPES OF CYBERCRIME

1. HACKING & ACCOUNT THEFT

When someone breaks into your accounts - social media, email, or even school platforms - without permission.

Examples: Someone resets your password and posts as you online, or steals your game account.

Classroom Activity: Discuss what would happen if your social media account was hacked. How could you recover it?

2. PHISHING & SCAMS

Fake messages, emails, or websites that trick you into giving personal information.

Examples: Messages claiming "You won a scholarship" or "Your account is suspended - click here."

Tip: Always check the sender's email and never click suspicious links.

3. CYBERBULLYING & HARASSMENT

Using online tools to threaten, shame, or intimidate someone.

Examples: Mean comments, spreading rumors, or sending threatening messages.

Activity: Role-play how to respond safely to a cyberbully.

4. IDENTITY THEFT & IMPERSONATION

Someone pretends to be you online to trick others or steal info.

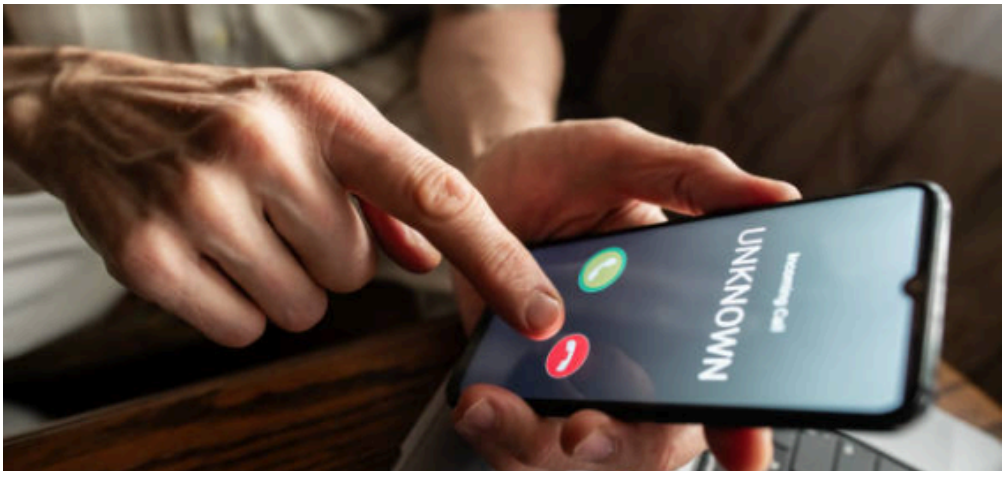
Examples: Fake profiles posting in your name, or tricking friends for money.

5. NON-CONSENSUAL IMAGE SHARING / SEXTORTION

Sharing private photos or messages without permission, often to threaten or blackmail.

Examples: A private photo is shared to embarrass or coerce someone.

Discussion Prompt: Why do you think this is a bigger risk for some students in Pakistan?



6. MALWARE & VIRUSES

Software that harms devices or steals information.

Examples: Apps or files that install viruses when opened.

7. ONLINE FRAUD & FINANCIAL SCAMS

Tricking people into giving money or financial details.

Examples: Fake online stores, donation scams, or investment fraud.

MINI TIP BOX:

- Think before you click, share, or download anything.
- Verify requests for personal info, even if they seem to come from friends.
- Keep your devices and apps updated to avoid malware.
- Report suspicious activity immediately.

Cybercrime Detective: Break students into groups and give each a scenario (like phishing, cyberbullying, malware). Ask them to identify the type of cybercrime, what the victim should do, and how it could have been prevented.

RED FLAGS AND PREVENTION

Cybercrime often starts small - an odd message, a strange friend request, or a link that doesn't feel right. These are your red flags. Learning to recognize them and knowing how to respond is the best way to stay safe online.

COMMON RED FLAGS

Suspicious Messages or Links

- Messages that ask for your password, personal info, or money.
- Links claiming "You won a prize!" or "Your account is suspended - click here."

Unexpected Friend Requests

- People you don't know sending friend requests or follow requests.
- Fake profiles trying to gain your trust.

Requests for Private Information

- Asking for your passwords, private photos, or school info.
- Even if the request comes from someone you know, pause and verify.

Strange Behavior Online

- Messages with threatening, shaming, or manipulative language.
- People pretending to be friends to trick you or steal information.

Shared Devices Risks

- Using a computer or phone that others can access can expose your accounts.

CLASSROOM ACTIVITY

Red Flag Detective: Give students 5–6 sample messages, friend requests, or posts (mix safe vs. suspicious). Ask them to identify red flags and explain what they would do.

PREVENTION TIPS

Think Before You Click:
- Don't click on links or download files unless you are 100% sure they're safe.

Keep Passwords Secret:
- Never share your passwords, even with friends or family.
- Use strong, unique passwords for different accounts.

Enable Security Features:
- Turn on two-factor authentication (2FA) on social media and email.
- Update apps and devices regularly to prevent malware.

Pause and Verify:
- If a message seems off, check with a trusted adult or teacher before responding.
- Don't feel pressured to reply immediately.

Report Suspicious Activity:
- Save evidence (screenshots) if you feel safe.
- Use trusted channels to report cybercrime- Unmask'd' chatbot or your school's support system.

Be Careful with Online Friends:
- Accept friend requests only from people you know and trust.
- Remember, fake profiles can look real. stay cautious.

Check App Permissions:
- Some apps ask for access to your contacts, camera, or microphone, only allow what's necessary.

Backup Your Data:
- Regularly save important files, photos, and school work offline or in a secure cloud account.

Strange Behavior Online
- Messages with threatening, shaming, or manipulative language.
- People pretending to be friends to trick you or steal information.

Shared Devices Risks
- Using a computer or phone that others can access can expose your accounts.

Regular Digital Check-Ups:
- Review your social media privacy settings every few months.
- Remove old apps, accounts, or permissions you no longer use.

Use Safe Devices:
- Log out from shared computers or public devices.
- Don't save passwords on devices others can access.

Protect Personal Information:
- Think twice before sharing your location, school info, or contact details online.
- Avoid posting sensitive personal content publicly on social media.

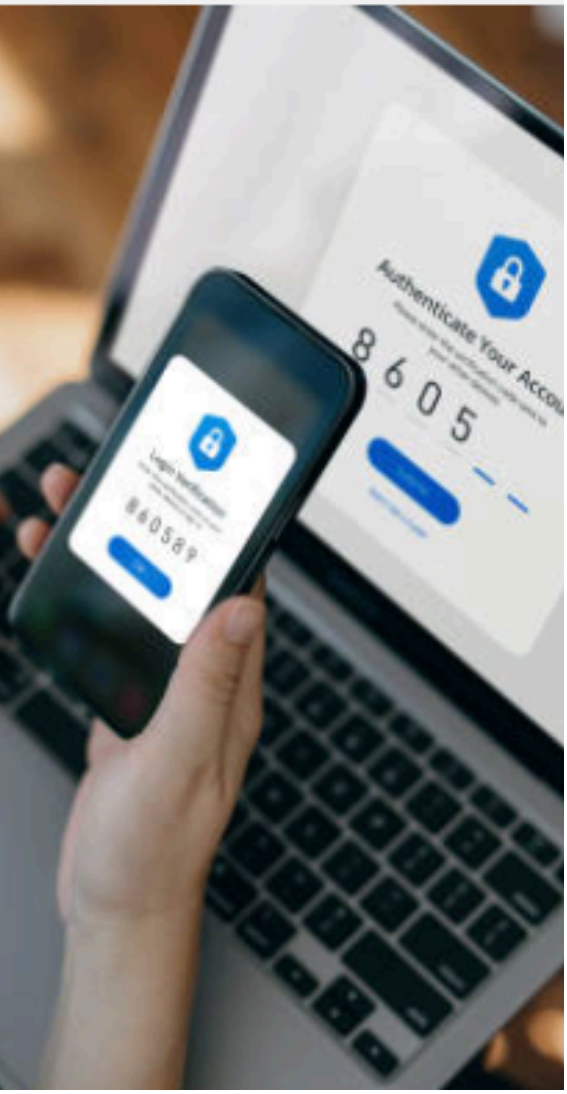
CLASSROOM ACTIVITY

Prevention Brainstorm: In small groups, students list 5 ways they personally keep their devices, accounts, and privacy safe.

THINK TWICE

BEFORE YOU CLICK!

- *Offer is too good to be true.*
- *Messages with urgency (“act now!”).*
- *Unknown links or attachments.*
- *Accounts asking for personal info.*
- *Inconsistent spelling/design.*



CYBER HYGIENE 101

1

Strong Passwords Are a Must
Use unique passwords for each account. Make them long, mix letters, numbers, and symbols.

2

Update, Update, Update
Always update your apps, devices, and antivirus software. updates fix security holes hackers might exploit.

3

Think Before You Click or Share
Hover over links to see the real URL before clicking. Ask: “Would I share this info in real life?” if the answer is no, don’t post it.

4

Manage Your Accounts & Privacy Settings
Regularly review social media privacy settings. Limit who can see your posts and personal info. Log out from shared devices or public computers.

5

Two-Factor Authentication (2FA) Is Your Best Friend
Adds an extra step when logging in to make it harder for someone to hack your account. Even if a password is stolen, 2FA can block access.

6

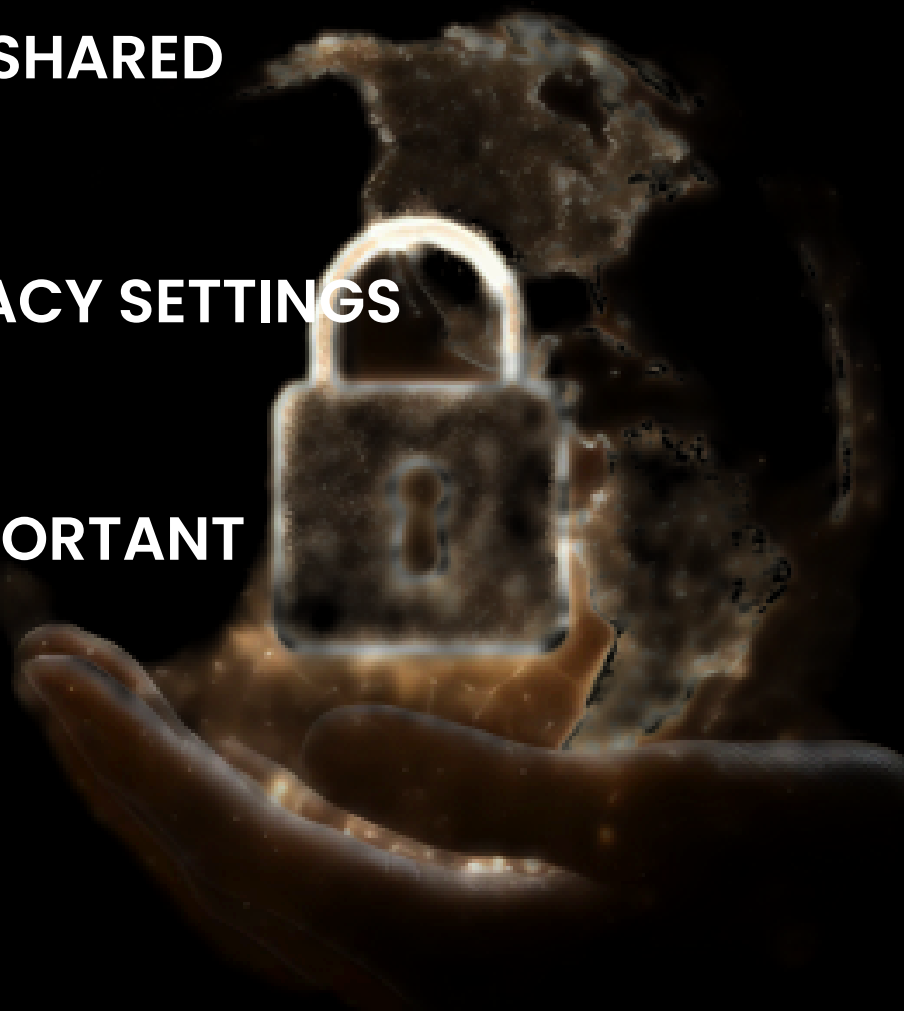
Beware of Unknown Contacts & Requests
Save important school work, photos, and files offline or in secure cloud storage. This protects you if a device is lost, stolen, or hacked.

7

Use Secure Networks
Avoid logging in to accounts on public Wi-Fi. If you must, use a VPN or trusted network.

YOUR DAILY DIGITAL SAFETY ROUTINE

- [ ] USE STRONG, UNIQUE PASSWORDS
- [ ] UPDATE YOUR APPS REGULARLY
- [ ] LOG OUT OF SHARED DEVICES.
- [ ] CHECK PRIVACY SETTINGS WEEKLY
- [ ] BACK UP IMPORTANT DATA



Your Legal Rights in Pakistan

Rafay Baloch

As someone who has spent years studying and working in cybersecurity, I understand how important it is for you to feel safe and protected online. Whether you're browsing social media, chatting with friends, or doing schoolwork, your rights matter. In Pakistan, the law is here to protect you.

I've spent years hunting bugs, reporting vulnerabilities to big companies like PayPal, Google, and Microsoft, and writing about ways people's privacy gets broken—not just because of software flaws, but because many laws, norms, and practices don't protect us equally. Growing up in Karachi, I saw how even small online harms—harassing messages, fake profiles, leaks—hit some people far harder. That's why knowing your legal rights isn't optional; it's essential.

Pakistan's Prevention of Electronic Crimes Act (PECA 2016) is one of the main tools you have. It says that no one should access your accounts without permission, harass you online, threaten you, impersonate you, or share your private photos or messages without your consent. PECA helps protect you from identity theft, fraud, online bullying, and other digital harms. But I know laws alone aren't enough—knowing when your rights are being violated, and how to use them, is just as important.

From my own work, I've seen people hesitate to report because they don't think what happened "serious enough," or they worry about shame, or simply don't know where to turn.

I remember finding an address-bar spoofing bug in Chrome/Firefox, getting recognized globally, and thinking: if I can discover that vulnerability, then you need to believe you can stand up for your safety too.

So here's my message to you: don't underestimate the power of knowing your rights. If someone harasses you online, you can save the evidence and report it under PECA. If someone impersonates you or shares your content without permission, you can demand action. And if you ever feel like you're alone, remember - you aren't. People like me, and platforms like Unmask'd, are here because your safety matters.

How To Report Cybercrime

One of the most important things to remember is this: you are not powerless online. If you face harassment, blackmail, hacking, or any other cybercrime, you have the right to report it and seek justice. Reporting may feel intimidating, but it is the first step in protecting yourself and others.

1

Stay Calm and Gather Evidence
Take screenshots of messages, posts, or images. Save links, usernames, and phone numbers. Don't delete conversations, even if they make you uncomfortable, they can be crucial proof.

2

Explore Reporting Options
You have multiple ways to take action in Pakistan:

1. National Response Center for Cyber Crime (NR3C – FIA)
   - The FIA (Federal Investigation Agency) handles cybercrime complaints. You can report online at: FIA Cybercrime Complaint Portal. Or email: helpdesk@fia.gov.pk. In emergencies, you can also visit the nearest FIA cybercrime wing office.
2. Helplines and NGOs
   - Digital Rights Foundation (DRF) Helpline: 0800-39393 (Mon–Sat, 9 AM–5 PM)
3. Unmask'd Toolkit
   - Our Legal Aid Chatbot explains your rights under PECA in simple Urdu/English and walks you through the reporting process. You can use the Impact Tracker to record incidents anonymously, which helps you keep a log if you decide to take action later.

3

Submit Your Complaint
When filing with the FIA:
Use your CNIC (or a parent/guardian's if you're under 18). Provide the screenshots, links, or other evidence you've collected. Explain clearly what happened and how it has affected you.

4

Follow Up
The FIA may contact you for more details. NGOs like DRF can help you understand updates and next steps. Remember: you have the right to confidentiality and respectful treatment during the process.

Don't Stay Silent - Report It

1. SAVE EVIDENCE
2. REPORT TO FIA
3. CONTACT DRF HELPLINE
4. USE UNMASK'D CHATBOT FOR GUIDANCE

RESOURCES AND HELPLINES

FIA Cybercrime Wing (NR3C)

Report cybercrimes directly.

📍 nr3c.gov.pk | ✉️ helpdesk@fia.gov.pk

Digital Rights Foundation (DRF) Helpline

Free support with legal guidance, tech help, and counseling.

☎️ 0800-39393 (Mon–Sat, 9 AM–5 PM)

Unmask'd Toolkit

Legal Aid Chatbot (PECA explained simply)

Impact Tracker (log incidents safely)

Resources for digital safety + emotional support

Madadgar Helpline

For women and children facing abuse (online or offline).

☎️ 1098

Police Helpline

In emergencies, dial 15.

Teacher's Guide: Using This Toolkit in Classrooms

This toolkit is designed to spark meaningful conversations about digital safety, not just deliver dry facts. As a teacher, you play a key role in creating a safe space where students feel comfortable learning and sharing. Here's how to use it effectively:

1. Set the Tone

- Begin by explaining why digital safety matters for everyone - boys and girls, teachers and students.
- Remind students that the classroom is a judgment-free zone. Everyone's experiences are valid.

2. Introduce Topics Step by Step

- Start with "Understanding Cybercrime" to build awareness.
- Move into "Types of Cybercrime" and "Red Flags & Prevention" with real-life examples.
- Use "Cyber Hygiene 101" as an interactive checklist activity.
- Wrap up with "Your Legal Rights" and "How to Report a Cybercrime."
- *Every new section includes classroom activities in italics, so you'll always have ready-made exercises and discussion prompts to guide your lesson.*
- *Midway through the toolkit, you'll also find printable posters and infographics inserted right after key topics. These can be displayed in classrooms, used as handouts, or incorporated into discussions for visual reinforcement.*

3. Encourage Participation

- Break students into small groups for role-plays (e.g., how to respond if someone sends a suspicious link).
- Use reflection prompts included in the toolkit to spark discussion.
- Allow space for anonymous sharing (students can write questions on slips of paper if they're shy).

4. Handle Sensitive Topics with Care

- Some students may share personal experiences. Acknowledge their courage and avoid judgment.
- If a case sounds serious, gently encourage them to speak privately after class and connect them to resources/helplines listed in the toolkit.

5. Connect Learning to Action

- Encourage students to save helpline numbers on their phones.
- Ask them to share one prevention tip with a family member at home.
- Consider inviting local experts (like IT teachers, digital rights advocates, or even former students working in tech) to speak.

6. Use Unmask'd Tools

- The Legal Aid Chatbot can be shown live in class to demonstrate how it simplifies PECA laws.
- The Safety Quiz makes a great icebreaker or end-of-lesson activity.
- The Impact Tracker can be introduced as an optional tool for students who want to log issues safely.

Reminder for Teachers!

You don't need to have all the answers. Your role is to guide students through discussion, show them where to find resources, and remind them they have rights. The toolkit is built to support you with content, prompts, and classroom activities already embedded in each topic.