



DIGITAL GUARD
Cybersecurity Awareness Initiative

THINK BEFORE YOU TRUST

AI makes scams look real.
Stay alert. Stay protected.

PUBLIC AWARENESS
GUIDE 2026



Scan to visit
DigitalGuard.info
and follow **@DigitalGuard**
on Facebook & Instagram
for cybersecurity awareness
resources.

FOLLOW US



/digitalguard

Together for a Safer Digital Pakistan



WHAT TO DO IF YOU'RE TARGETED

- 1 Stop all communication immediately.
- 2 Do not send money or share information.
- 3 Change passwords for affected accounts.
- 4 Inform your bank or mobile wallet provider.
- 5 Report the incident to relevant authorities.

REPORT CYBER CRIME



National Cyber Crime
Investigation Agency
(NCCIA)



Helpline: 1991



Website: nccia.gov.pk



Email: helpdesk@nccia.gov.pk

FIA COMPLAINT PORTAL



Scan to file a cybercrime
complaint through the
FIA Complaint Portal.



Remember:

Being targeted does not
mean you failed. Reporting
helps protect others too.



**AMAL
ACADEMY**

This awareness campaign is developed
under the Amal Academy Fellowship Program.



AI-POWERED THREATS IN 2026

Artificial Intelligence is changing how scams work.
Criminals can now create fake messages,
voices, and identities within minutes.



1. DEEPFAKE VOICE CALLS

Scammers copy a family member's voice
and ask for money or urgent help.



2. AI-GENERATED PHISHING MESSAGES

Fake emails and messages now look
more professional and convincing.



3. FAKE AI CUSTOMER SERVICE CHATBOTS

Fraudsters create fake support
accounts that steal information.



4. SYNTHETIC FAKE IDENTITIES

AI can create realistic people
who do not exist.



GOLDEN RULE

Always verify requests through a
trusted phone number before taking action.

**STAY ALERT.
STAY SECURE.**



SHARE THIS GUIDE

Help protect your family, friends
and community by sharing
cybersecurity awareness.



TYPES OF CYBER FRAUD

1



PHISHING

Fake messages trick you into sharing passwords or banking details.

Example: "Your account is blocked. Click here immediately."

2



SIM SWAP

Criminals transfer your number to another SIM card to gain access to your accounts.

Example: Your phone suddenly loses network service.

3



ONLINE SHOPPING SCAMS

Fake sellers advertise products they never deliver.

Example: You pay online but receive nothing.

4



ROMANCE SCAMS

Scammers build trust and later ask for money.

Example: An online friend requests emergency funds.

5



INVESTMENT & CRYPTO FRAUD

Fraudsters promise guaranteed profits with little risk.

Example: "Double your investment in one week."

6



JOB SCAMS

Fake employers request fees or personal information.

Example: "Pay a registration fee to secure your job."



HOW TO PROTECT YOURSELF



1

USE STRONG PASSWORDS

Create unique passwords for every account. Avoid using personal information.



2

ENABLE TWO-FACTOR AUTHENTICATION

Add an extra security step beyond your password.



3

THINK BEFORE YOU CLICK

Check links carefully before opening them. Avoid unknown links and attachments.



4

VERIFY CALLERS

Confirm requests using a trusted contact method.



5

SHOP SAFELY

Buy only from trusted websites and sellers. Check reviews and ratings.



6

KEEP DEVICES UPDATED

Updates fix security weaknesses and improve protection.



7

TALK TO YOUR FAMILY

Discuss scams regularly with parents, children, and relatives.



AWARENESS IS YOUR STRONGEST DEFENSE.



RED FLAGS — WARNING SIGNS

Stop immediately if you notice any of these:



Urgent requests for money

Scammers create pressure to make you act fast.



Requests for OTP codes

No genuine organization asks for OTP or PIN.



Too-good-to-be-true offers

If it sounds unbelievable, it probably is.



Unexpected prize notifications

You didn't enter any draw or contest.



Pressure to act quickly

Scammers rush you so you can't think clearly.



Unknown links or attachments

They may install harmful software.



Requests for banking details

Banks never ask for your full details.



Calls claiming to be from officials

Always verify their identity first.



FOLLOW US



/digitalguard

Stay informed. Stay secure.
Stay one step ahead.

**STAY ALERT.
STAY SECURE.**



GOLDEN RULE

Always verify requests through a trusted phone number before taking action.

FIA COMPLAINT PORTAL



Scan to file a cybercrime complaint through the FIA Complaint Portal.