



CYBER BULLETIN

DIGITAL ARREST CHRONICLES

RANSOMWARE ATTACK 1.



FAKE ARREST THREATS

TARGET: Individuals, businesses, government agencies.

IMPACT: False claims that files contain illegal content (e.g., child pornography or pirated material), leading to fear of legal action.

MITIGATION: Use up-to-date antivirus software and firewalls. Regularly back up data to a secure cloud or offline storage. Avoid clicking on suspicious email links or attachments.

LAW ENFORCEMENT SCAM 2.



IMPERSONATION SCAM

TARGET: General public, especially those unfamiliar with digital security.

IMPACT: Financial loss from paying a fake "fine" or "legal fee" to avoid arrest.

MITIGATION: Always verify any communication from law enforcement by contacting them directly through official channels. Do not provide personal or financial information over the phone or email.

TAX OR LEGAL AUTHORITY 3.



IMPERSONATION SCAM

TARGET: Taxpayers, business owners, elderly people.

IMPACT: Victims are led to believe they owe taxes or fines and will be arrested unless they pay immediately.

MITIGATION: Always verify tax-related communications through official government websites or phone numbers.

SOCIAL MEDIA 4.



IMPERSONATION SCAM

TARGET: Social media users, particularly high-profile individuals or their friends/family.

IMPACT: Attackers impersonate friends or family and claim they are in legal trouble or under arrest, requesting immediate funds for bail or legal fees.

MITIGATION: Always verify any urgent request for money or personal details directly with the person, via a phone call or official message.

ONLINE DATING 5.



FAKE ARREST THREATS

TARGET: Individuals seeking online relationships.

IMPACT: Attackers build fake romantic relationships, then fabricate a crisis (e.g., arrest or legal trouble) to extort money.

MITIGATION: Be cautious of requests for money from someone met online, especially if they are "in trouble."

PHISHING SCAM 6.



LEGAL ARREST THREATS

TARGET: General public, especially those with limited cybersecurity knowledge.

IMPACT: Victims receive fake emails claiming they are under arrest or face criminal charges, with a link to "settle" the case by entering personal or financial information.

MITIGATION: Always check the email sender's address and be cautious of any unsolicited emails that threaten arrest.



इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी विभाग
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY



CYBER SECURITY
POSTER OF THE DAY

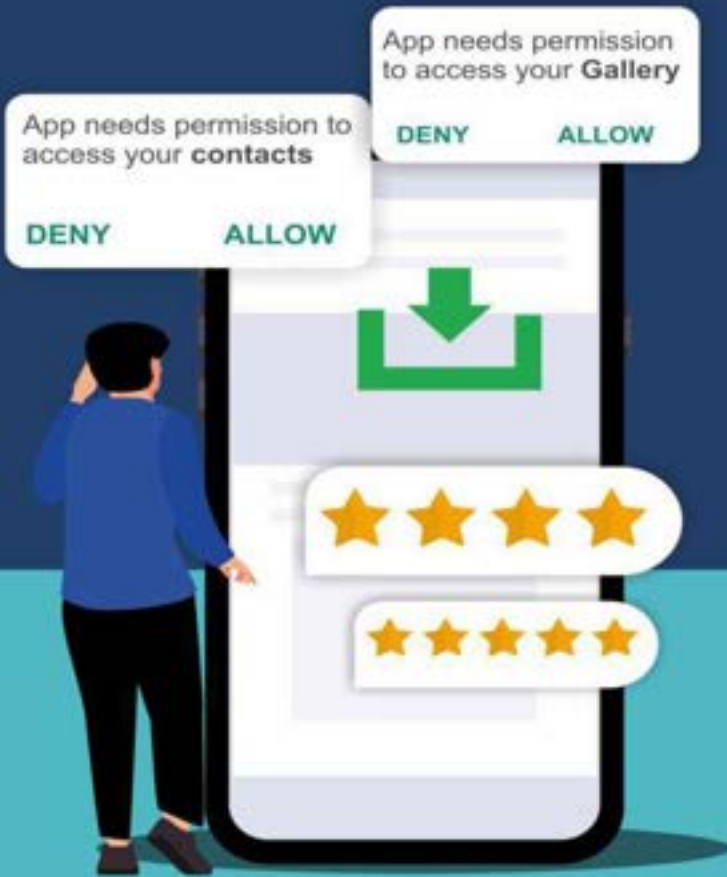


← Cyber Ethics

Before downloading an app, read reviews and check permissions

Check reviews and see what kind of data the app collects

#BeSafeFrom AppTrap



Supported by



CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS

Mr. SHUBHAM KUMAR | Mr. FAIZAN MAHMOOD

STUDENTS COORDINATORS

MOHAMMAD FARHAN | SIDRA SIDDIQUI | ELMA SHARIQ | ADEEBA KHATOON
ANSHA ALVI | ARSHI KHAN

Prof. (Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application