Safe Internet Usage Practices:

IIIT Delhi users are requested to carefully read and follow the following internet usage advisory to ensure safe and secure browsing practices. Adhering to these guidelines will help protect personal and institutional data from potential online threats.

Phishing: Emails or messages that appear to be from legitimate sources (e.g., banks, social media platforms) requesting personal information or login credentials.

Emails from Known Name :-
Be cautious of scam emails that appear to originate from someone you know. These emails often use the name of a trusted contact and urgently request your assistance, usually in the form of money. Scammers rely on impersonation tactics to pressure you into responding quickly without verifying the authenticity of the request.
Always verify such emails by checking the sender's email ID or directly contacting the person through a reliable method, such as a phone call or face-to-face conversation, before taking any action.

Smishing: Similar to phishing, but via text message.
Vishing: Voice phishing, where scammers call pretending to be from legitimate organizations.
Ransomware: Malware that encrypts your files and demands a ransom to unlock them.
Online Shopping Scams: Fake websites or offers that trick you into purchasing counterfeit or non-existent goods.

Phishing Scams
Fake job offers: Scammers often send out emails offering high-paying jobs that require you to provide personal information or upfront payments.
Fake tech support calls: You receive a call claiming to be from a tech support company, warning you about a virus on your computer and offering to help fix it for a fee.
Fake charity donations: Scammers impersonate charities to solicit donations, often using urgent messages about a crisis.

Social Engineering Scams
Impersonation scams: Scammers create fake profiles on social media platforms to befriend you, then ask for money or personal information.
Romance scams: Scammers build romantic relationships online to gain your trust and eventually ask for money.
Extortion scams: Scammers threaten to release embarrassing or damaging information about you unless you pay a ransom.
Financial Scams
Investment scams: Scammers offer high-yield investments with little to no risk.
Cryptocurrency scams: Scammers promote fake cryptocurrency investments or offer to sell you cryptocurrency at a discount.
Check scams: You receive a check in the mail and are asked to deposit it and send a portion of the funds back.

UPI Scams: A stranger accidentally transfers money to your account and wants it back? Possibly a scam
Smishing Text: You have won a free iPhone! To claim, reply with your name and address.
Online Shopping Scams
Fake online stores: Scammers create fake websites that look legitimate to sell counterfeit or non-existent goods.
Overpayment scams: You receive a payment that is more than the agreed-upon amount and are asked to return the difference.
Shipping scams: You pay for an item but never receive it.

Advisory for Users :

1. Each user is responsible for taking reasonable care for the security of his or her IIITD account and password. One should under no circumstances share
his or her password with anyone.

2. Students must always log out of their own account at the end of each class session.

3. Do not disclose sensitive information such as bank account details, passwords, OTP on email or on phone.

4. Don’t open suspicious attachments or click unusual links in messages.
They can appear in email, tweets, posts, online ads, messages, or attachments, and sometimes disguise themselves as known and trusted sources.

5. Avoid visiting sites that offer potentially illicit content. Many of these sites install malware on the fly or offer downloads that contain malware. Use a
modern browser like Mozilla Firefox, Google Chrome/Chromium, Microsoft Edge which can help block malicious websites and prevent malicious code
from running on your computer.

6. Please scan USBs or other external devices to avoid infection by malware and viruses, ensure that all external devices either belong to you or come from
a reliable source.

7. Please avoid using any free WiFi network, so as to prevent inadvertent compromise of user/account privacy,

Be Skeptical: Never click on links or open attachments in unsolicited emails or messages.
Verify Information: Double-check the sender's address and any links before clicking.
Use Strong Passwords: Create unique, complex passwords and avoid sharing them.
Enable Two-Factor Authentication: Add an extra layer of security to your online accounts.
Keep Software Updated: Regularly update your operating system and software to patch security vulnerabilities.
Be Cautious Online: Avoid sharing personal information on social media or public forums.

Remember: Always be cautious of unsolicited emails, messages, or calls, especially those asking for personal information or money. If something seems suspicious, do your research and verify the information before taking any action.

If you suspect a scam, don't respond or click on any links. Contact the organization directly using a phone number or email address you know is legitimate.

By staying informed and practicing safe online habits, you can significantly reduce your risk of falling victim to cyber scams.