Cyber Suraksha Dishanirdesh vol. 25

national health authority

Online Fraud or Internet Fraud – How to recognize it and safeguard our information

How an online fraud works?

Scam or Phishing: Convincing an individual of something which is not true.

Spam: Constantly bombarding one with messages and emails.

Identity Theft: The thief pretends to be you by stealing credit card details or account passwords.

Spyware, Hardware additions: Adding something (hardware or software) which can steal one's key pattern.

WHAT IS INTERNET FRAUD?

Internet fraud is a type of cybercrime fraud or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, information, and identity.

01

Spam is a generic term used to describe electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. They attempt to trick one into divulging bank account or credit card details

02

Spyware is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user.

03

Largely online crime is centered on **identity theft** which is part of identity fraud and specifically refers to the theft and use of personal identifying information of an actual person.

04

Phishing involves using a form of spam to fraudulently gain access to people's online banking details

Report all security incidents to it.securityincident@nha.gov.in

Cyber Suraksha Dishanirdesh vol. 25

national health authority

Mobile phones/smartphones have become a necessity today, hence, the security of the same is of utmost importance…

- ✓ Phone service & text messaging
- ✓ Personal email
- ✓ Scheduling appointments & reminders
- ✓ Online shopping, banking & bill paying
- ✓ Accessing social websites
- ✓ Listening music & watching videos
- ✓ Playing online games

What are the Attack Vectors?

Untrusted apps may contain Malware / Spyware that can steal your Information and causes system instability.

Loss theft / unauthorized access to mobile devices can lead to sensitive data (financial and personal) stored in mobile device.

Wireless Interface: An attacker operating his own hotspot with a corresponding name (e.g. free internet, telecom or hotel) can imitate a bogus access and is thus able to directly read a victim's data that has been sent or received over this hotspot.

How to Protect ourselves?

✓ **Your PIN code must be truly random. Never use your date of birth, phone number, or ID number. Use biometric auth (fingerprint, voice, or face) if device supports it**

✓ **Do not escalate privileges. Rooting or jailbreaking a mobile device opens up access to the device file system and disables protection mechanisms.**

✓ **Do not connect your mobile device to untrusted PCs or charging stations.**

✓ **Do not trust third-party mobile app stores. Suspicious software (such as allegedly "cracked" free versions of commercial applications) can contain malicious code**

✓ **Do not open links received from unknown senders in SMS messages and chats. Never confirm requests for installation of third-party software on your smartphone.**

✓ **Update your OS and applications regularly. If you have rooted or jailbroken your mobile device, remember that it may not update automatically.**

Report all security incidents to it.securityincident@nha.gov.in