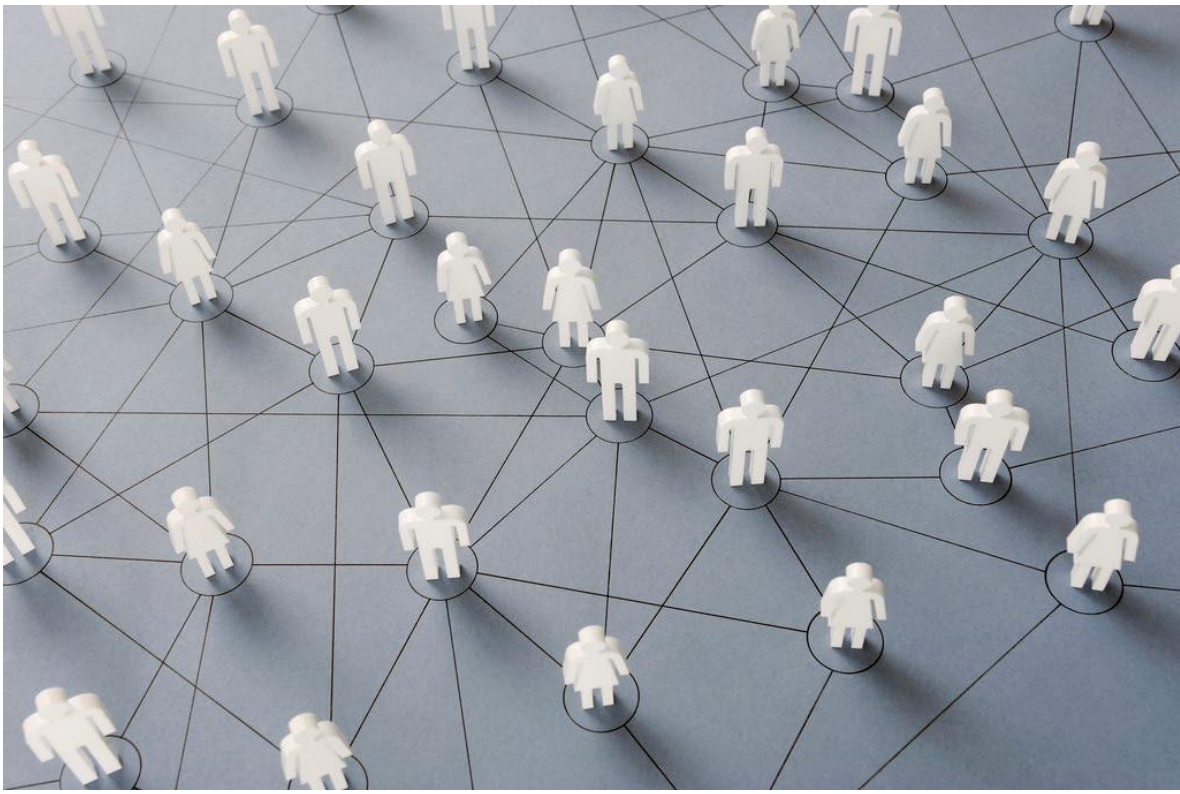
Niyo Money

Cyber Security Awareness For Niyo Money Users

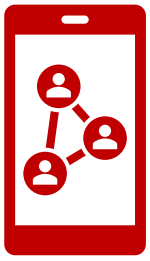


What's Inside?

Disclaimer:

Niyo Money

Trending Social Media Frauds



Social Media has become an integral part of our lives. It is the new way of communicating, sharing and informing people about the events in our lives. We share our day to day lives on social media in the form of self and family photographs, updates on our locations/whereabouts, our views/thoughts on prevalent topics etc. One can understand the entire history of an individual through their social media profile and can even predict future events based on patterns in the past. This poses a threat to an individual as unwanted access to social media profile can cause loss of information, defamation or even worse consequences such as physical/sexual assault, robbery etc. Hence, protection and appropriate use of social media profile is particularly important. Let us look at some examples of social media frauds:

Sympathy Fraud - The attacker becomes friends with the victim on social media. The attacker gains trust by frequent interactions. The attacker later extracts money/harms the victim.

Romance Fraud - The attacker becomes friends with the victim on social media. Over a period, the attacker gains victim's affection. The attacker later exploits the victim physically, financially and/or emotionally.

Cyber Stalking - Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), messages posted on a website or a discussion group. A cyber stalker relies upon the fact that his/her true identity is not known in the digital world. A cyber stalker targets the victim with threatening/abusive messages and follows them/their activities in the real world.

Cyber Bullying - Cyber bullying is bullying that takes place over digital devices. Cyber bullying can occur through SMS, social media, forums or gaming apps where people can view, participate or share content. Cyber bullying includes sending, posting or sharing negative, harmful, false content about someone else. The intention is to cause embarrassment or humiliation. At times, it can also cross the line into unlawful criminal behavior.

TIPS

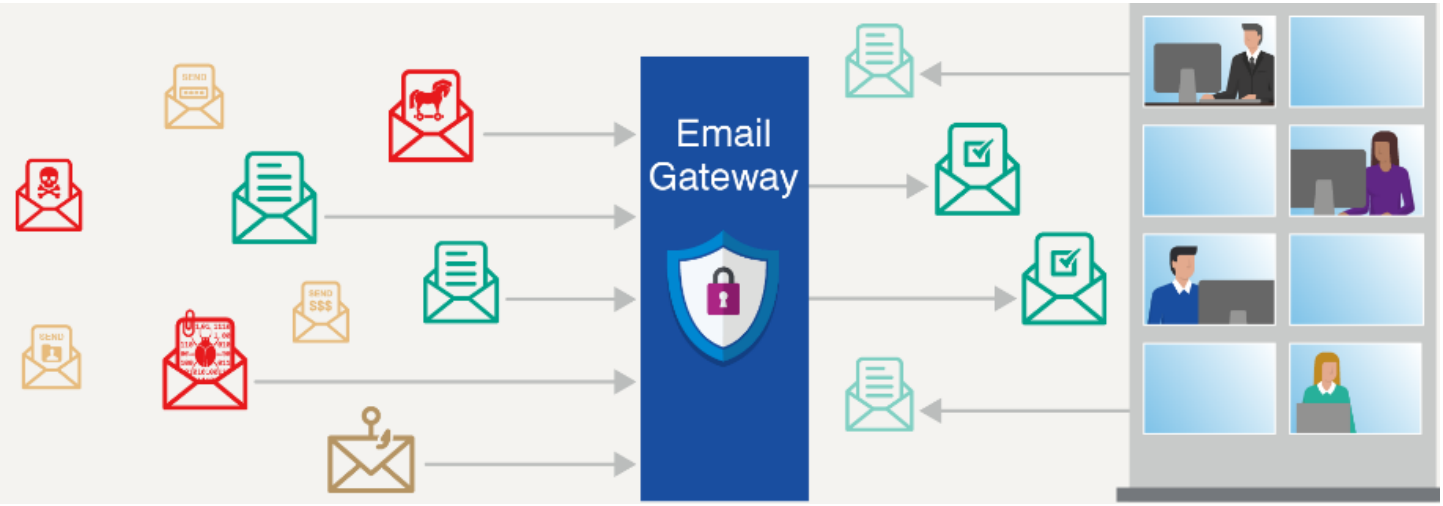
- Be careful while accepting friend request from strangers on social media. Cyber criminals often create fake social media profile to befriend potential victims with an intention to harm them.
- Do not share personal details or get into financial dealings with an unknown person whom you have met on social media platform.
- Restrict access to your profile. Social media sites offer privacy settings for you to manage who can view your posts, photos, send you friend request etc.
- Ensure your personal information, photos and videos are accessible only to your trusted ones.
- Be careful while uploading your photos on social media which show your location or places you frequently visit as cyber stalkers may track your daily life.
- Keep family/friends informed, in case you plan to meet a social media friend. Always plan such meetings in public places.

Niyo
Money

Email Frauds & Security Tips

In today's modern and fast moving technology, it is important to protect your communication channels. An email fraud involves any such email that is intended to defraud someone for personal or professional gains. Also called a phishing scam, email scam messages usually trick you into making payments using look-alike websites and fraudulent emails.

Email fraud is intentional deception for either personal gain or to damage another individual by means of email. Almost as soon as email became widely used, it began to be used as a means to defraud people. Email fraud can take the form of a "con game", or scam. Confidence tricks tend to exploit the inherent greed and dishonesty of its victims. The prospect of a 'bargain' or 'something for nothing' can be very tempting. Email fraud usually targets naive individuals who put their confidence in schemes to get rich quickly. These include 'too good to be true' investments or offers to sell popular items at 'impossibly low' prices. Many people have lost their life savings due to such email frauds.



Some perpetrators may even end up convincing you to click on a fraudulent link that prompts them to fill out a form. Such forms are made to look exactly like a genuine job application form demanding users to enter their personal details. Sometimes, a victim's personal data is sold off to third parties for a hefty sum, or as a part of a larger network of identity theft.

Let us look at some day to day example on how emails can be used for cyber frauds:

Lottery Scam - A lottery scam is also a type of an advance fee fraud. In this, an individual receives a sudden, unsolicited email about winning a hefty sum of money in a lottery. The winner is then asked to contact a 'claims agent' to receive the sum assured to him. The victims are convinced to pay a 'processing fee' or 'transfer charge', which they innocently end up paying! Unfortunately, the lottery award is never received by them. Some lottery scams are very difficult to be identified even by the most well-read. These are the ones in which perpetrators deceive victims using names of actual lottery organizations or other such legitimate companies.

Online Dating/ Matrimonial Scam - Online dating/ matrimonial platforms have emerged as a popular platform for the current generation to seek a suitable match. However, this has also made such platforms a flourishing place to trap innocent users of online dating and matrimonial sites. Online dating scams usually start from an online dating or matrimonial platform wherein the perpetrator befriends the victim. Eventually, the conversation is moved off the dating

site to a personal email or an online or social media chat room. One commonly used method in this email scam is when the perpetrator pretends to be based out a foreign nation. They then take advantage of the victim's trust by demanding money under various pretexts. Some commonly used tricks include asking for money to clear customs duty for expensive gifts, treatment of a family member, or to salvage a sinking business abroad.

Job Scam - Job scam is also one of the common types of email scams in India. This is because each day lakhs of job-seekers upload their resume on several job search engines in India. The scammer chooses a particular profile and sends a spoofed email with a fake offer letter to the victim. The offer letters often bear the logo of reputed organizations and promise a hefty salary and remuneration. A common method to cheat job seekers in such email scams is to request them to pay an advance fee to attend the interview or secure the job. In the already saturated job market in India, desperate job seekers end up falling for such phishing scams.

Sick Baby Scam - The sick baby scam is another popular phishing scam across the world in which sympathy for a sick baby is used to defraud people. In this form of an email scam, one receives an email containing a photograph of a sick baby or child. It also contains a message from the 'fake' parents requesting financial help to bear the child's medical expenses. Such emails are circulated as a chain, requesting people to either make a small donation or forward the message to their friends. And as is expected, most fall for the helpless little child and end up clicking on the link provided or making a donation to the conman. Please remember that sharing an email or post can never equal donations! No website or social media platform shall donate money based on the number of times a post is shared.

TIPS

- Delete Unwanted/Suspicious Emails: Deleting unwanted emails is one of the best ways to avoid email frauds. Do remember that a genuine and legitimate enterprise shall never bombard with your continuous information through emails.
- Never Believe in Promises of Prizes or Money: Remember that no one really cares to give away enormous rewards as a social service! Please dismiss any such email that promises free rewards or monetary benefits.
- Don't give in to Request for Donations: A sick child, a natural disaster, and a hapless family with insufficient funds for medical treatment and so much more. Conmen use a number of such tactics to pull the emotional strings and demand for donations. Please do not pay heed to such requests. Instead, donate to legit charities such as the Red Cross.
- Avoid Sharing Personal Information: Any email demanding your personal information such as your Unique Identity Number, bank details, family information etc. should ring a warning bell in your head. Irrespective of what they promise, please mark the email as a spam and exercise caution.
- Don't Click on Suspicious Links: Exercise extra caution before clicking on a suspicious link in an email. Even if it 'seems' to be from a legitimate company, please do your background check before clicking on a link. Be aware of look-alike login pages or forms that require you to fill in your personal information.

Niyo
Money

Mobile Application Security

With the increase in the use of smartphones and the consequent rise in the use of mobile applications, associated security risks have also increased. The number of mobile transactions has increased four times in the last couple of years, and now, cyber criminals are targeting mobile users to extract data and money.

Mobile applications are widely used not only for entertainment but also for ease and convenience to perform day-to-day tasks such as bill payments, bank accounts management, service delivery etc. As a result, these applications are more prone to cyber-attacks. Users need to be aware of such attacks on commonly used mobile applications such as digital payment applications and gaming applications.

Let us look at some day to day example on how mobile applications can be used for cyber frauds.

Cyber-attacks using Infected Mobile Applications - People become habitual users of certain mobile applications. As a result, they ignore security warnings. Fraudsters use this to attack the victim by infiltrating through such popular mobile applications. They infect the applications with malicious software, called Trojan. This Trojan can get access to your messages, OTP, camera, contacts, e-mails, photos etc. for malicious activities. It can also show obscene advertisements, sign users up for paid subscriptions or steal personal sensitive information from the mobile etc.

TIPS

- Always install mobile applications from official application stores or trusted sources.
- Scrutinize all permission requests thoroughly, especially those involving privileged access, when installing/using mobile applications.
- For example, an entertainment application may not need your contact details access.
- Regularly update software and mobile applications to ensure there are no security gaps.
- Beware of malicious applications or malicious updates in existing applications.
- Clear all the data related to the malicious application and uninstall it immediately.

Story on Cyber-Attacks using Infected Mobile Applications

Maria and Shalini are housewives who use a mobile app to for free entertainment.

Maria: This app gives free entertainment without any paid subscription?

Shalini: Yes, I can watch movies, TV shows, etc. at free of cost.

Maria: But I read that this app is infected with malware. It shows intrusive ads and steal your personal/ financial details. It has even been removed from Google Play Store.

Shalini: But I think it will not affect my phone plus this app is extremely useful for me. I will not uninstall it.

(After a few days)

Shalini notices weird sounds from her phone. She realizes that her phone has started showing intrusive advertisements. She feels embarrassed to have opened such ads in front of her colleagues.

Maria: Don't worry, it's not your mistake. Don't feel embarrassed.

Shalini: It is. I should have uninstalled this app when I had the chance. Shalini regrets that she ignored the warnings and continued using an infected mobile application.

Niyo
Money

Online Financial Frauds

Nowadays, all financial services had shifted online. Services like investments in wealth market, buying insurance, banking services viz. retrieving account statement, funds transfer to other accounts, requesting a cheque book, preparing demand draft etc. can all be done online. Most of these services can be done sitting at home without physically visiting the financial service provider. As the services are shifting towards online platforms, cyber frauds related to financial services are also increasing. Just like we protect our locker full of jewellery with a lock and key, we must protect our online financial services account with strong passwords. If the key is stolen, then the jewellery will be stolen. Similarly, if the password is stolen, then the money in the online financial accounts will be stolen. Hence, protection of such financial accounts with strong passwords becomes highly essential.

Let us look at some examples of online financial fraud.

Applications related attacks – Financial service application have become very common in today's life. However, they do pose a threat if the account is hacked.

Hacking of financial account due to Weak Password - In this type of attack, the attacker hacks into the victim's account by using a program to guess commonly used passwords. Once the account is hacked, the attacker can steal money or perform an illegal transaction in order to defame or frame the victim.

Hacking of Multiple Accounts due to same password - If same password is used for multiple accounts, then hacking of one account may also lead to hacking of other accounts.

TIPS

- Never share your mobile unlocking PIN or passwords with anyone.
- Make the passwords stronger by combining letters, numbers and special characters.
- Keep updating your password periodically.
- Register your personal phone number and e-mail with your financial service providers and subscribe to notifications. These notifications will quickly alert you on any transaction and the unsuccessful login attempts to your financial accounts.
- Always review transaction alert received on your registered mobile number and reconcile it with your financial activity.
- Use a different password for each of your financial accounts and devices.
- Always keep a maximum transaction limit for your financial account.
- Secure your applications with strong password and 2-step verification (such as OTP), even for transactions

Niyo
Money

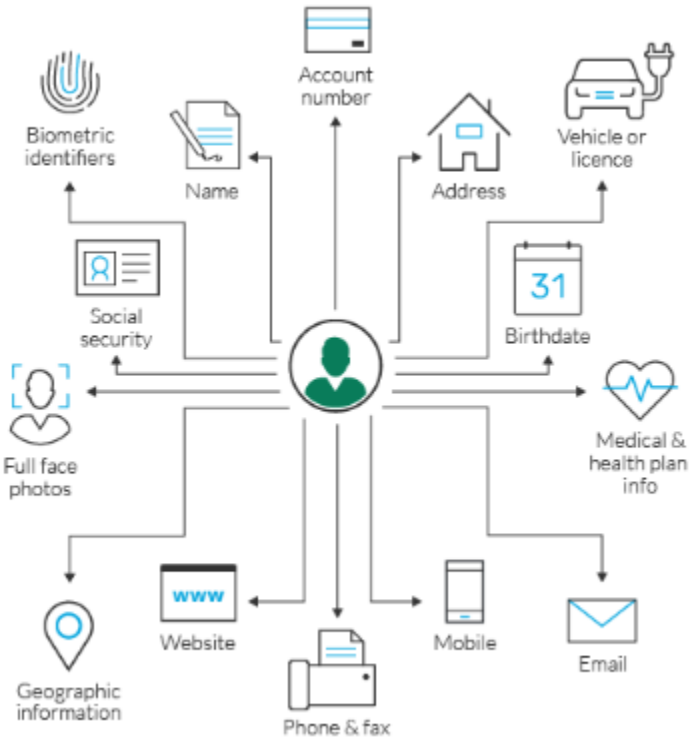
Importance of Data Security & Privacy

Data Security refers to the handling of sensitive personal data, also called "personally identifiable information" (PII). PII may include (but not limited to) Permanent Account Number (PAN), health records, and financial data, including your Aadhaar details, credit/debit/ prepaid card details, bank account credentials, etc. Keeping private data and sensitive information safe is paramount. If items like financial data, healthcare information, and other personal data get into the wrong hands, it can create a dangerous situation. The lack of access control regarding personal information can put you at risk for fraud and identity theft.

Advanced technologies have changed the modern way of life. The internet provides us with many benefits. Be it communicating with friends, searching for information, doing banking transactions, availing online services, finding job, finding life partner or even running entire businesses. The internet touches almost all aspects of our lives. However, it also makes us vulnerable to a wide range of threats.

New and powerful cyber-attacks are striking the internet regularly. A minor lapse in managing our digital lives can open the door to cyber criminals. Cyber criminals can steal our money or damage our reputation. According to a study by a leading industry research organization, 90% of all cyber-attacks are caused by human negligence. Therefore, data security and privacy are important for everyone today.

We must be vigilant while making use of technology to reduce the risk of cyber threats.



Always adhere to PII's simple privacy principles:

- **Notice –** What PI is being collected and for what purpose?
- **Consent & Choice –** Whether explicit consent is asked from you before collection of PII?
- **Use Limitation –** PII collected are used only for limited purposes?
- **Accoountability –** PII collected is not shared with any third party/ service providers?

Niyo Money

Where to Report Cyber Frauds?

1. Visit the nearest police station immediately.
2. To report cybercrime complaints online, visit the **National Cyber Crime Reporting Portal**. This portal can be accessed at **https://cybercrime.gov.in/.** In this portal, there are two sections. One section is to report crimes related to Women and Children (where reports can be filed anonymously as well). Another section is to report other types of cybercrimes. You can also file a complaint offline by dialling the helpline number **155260**.
3. In case you receive or come across a fraud SMS, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on **Maharashtra Cyber's** web portal by visiting **www.reportphishing.in**
4. Refer to the latest advisories which are issued by **CERT-IN** on **https://www.cert-in.org.in/**
5. Report any adverse activity or unwanted behavior to **CERT-IN** using following channels **E-mail: incident@cert-in.org.in Helpdesk:** +91 1800 11 4949 Provide following information (as much as possible) while reporting an incident.
    - Time of occurrence of the incident
    - Information regarding affected system/network
    - Symptoms observed

Niyo Money

General Safety Tips

1. Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.
2. Protect systems/devices through security software such as anti-virus with the latest version.
3. Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.
4. Keep Personal Information Professional and Limited
5. Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone.
6. Do not share your financial account passwords, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the financial service provider.
7. Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).
8. Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.
9. Be Careful What You Download
10. Always use virtual keyboard to access financial account facility from public computers; and logout from financial accounts portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online financial activity.
11. Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.
12. Make Online Purchases From Secure Sites
13. Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.
14. Be Careful What You Post on Social Media
15. Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/block/trace a phone using the IMEI code, in case the cell phone is stolen.
16. Be Careful Who You Meet Online
17. Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.
18. Do not save your card or financial account details in your wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.
19. If you think you are compromised, inform authorities immediately.

Remember India is going digital and so does evils, stay safe in cyber space.

Thank You

Niyo Money