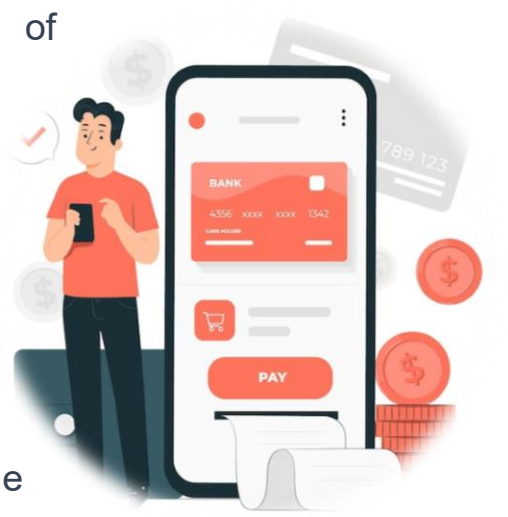
राष्ट्रीय डिज़ाइन संस्थान, असम
National Institute of Design, Assam

"Patch the leaks before the online ship takes on water, an ounce of prevention is worth a pound of cure."

Welcome to the November 2023 edition of our Cyber Security and Awareness newsletter! This month, we explore the various forms of **ONLINE Banking** and **Mobile App Frauds** and share essential insights on safeguarding yourself from digital threats. Our newsletter is your go-to resource for staying informed about the latest trends, threats, and strategies that define the dynamic realm of digital security. From in-depth articles on emerging cybersecurity technologies to actionable tips for fortifying your online presence, this edition is crafted to equip you with the knowledge required to navigate the cyber world with confidence.

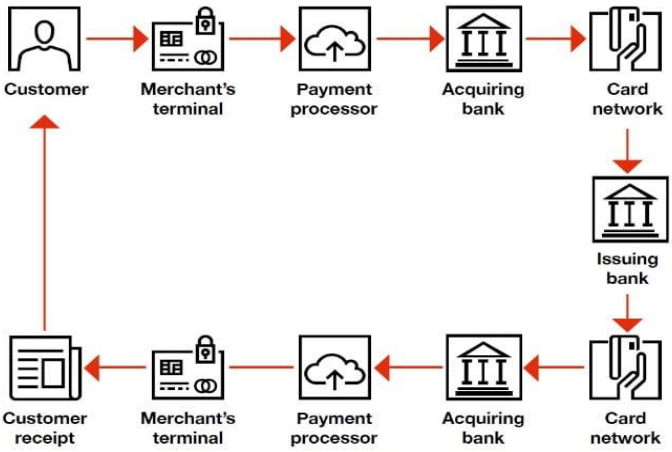
ONLINE BANKING FRAUDS

The surge in digital payments in India during the COVID-19 pandemic can be attributed to several factors. Innovations in the payments sector, coupled with regulatory support, the widespread availability of smartphones, and affordable mobile internet access, have collectively driven the substantial growth of digital transactions. Payment service providers, bolstered by new entrants and increased investments, have been pivotal in offering an improved and seamless user experience at competitive rates. This has not only facilitated the widespread adoption of digital payments but has also contributed to the evolution of a more robust and user-friendly digital payments landscape in India.



Users have multiple options for digital payments such as cards, wallets, Unified Payments Interface (UPI), mobile banking, QR code and various other methods.

Fraud in digital payments is driven by multiple factors such as local payment behaviour, customer awareness, security of payment systems, the regulatory environment, maturity of the payments domain, technical advancements and economic development of the country.



The payments ecosystem comprises multiple stakeholders such as banks, networks, payment gateways, channels, sellers, merchants, customers, and buyers, which interact with each other. These stakeholders may have risks associated with them.

For example, a single payment from a customer to a merchant involves multiple stakeholders in the payments process flow. When the customer pays the merchant,

the relevant information is passed on from the merchant payment gateway and processor to the customer’s issuing bank, through the card association network. Once the customer’s issuing bank authorises the transaction and deems it valid, the payment processor completes the transaction.

During this process, frauds can be perpetrated at any stage. Some common techniques and tricks used by the fraudsters in perpetrating these frauds across the payment’s ecosystem have been detailed in the following section.

Case Study 1: Phishing Banking App

Alice, a regular banking app user, received an email claiming a mandatory update for her mobile banking app. The email provided a link, seemingly from her bank, directing her to download the "updated" app.

Trusting the email, Alice clicked the link and downloaded what appeared to be her bank's official app. Unbeknownst to her, this was a phishing app designed to steal her login credentials. When Alice logged in, the attackers gained access to her account information.

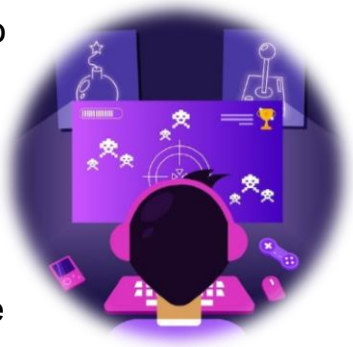
The impact was that Alice's sensitive banking details were compromised, leading to unauthorized transactions and potential identity theft.

Lesson Learned: Always update apps directly from the official app store or the official website of the service provider. Legitimate organizations rarely ask users to update apps via email links.

Case Study 2: Malicious Gaming App

John, an avid mobile gamer, found an exciting new game advertised on social media. The game promised unique features and bonuses, so John eagerly downloaded it from a third-party website.

Unknown to John, the gaming app contained malware that sought access to his contact list, messages, and device information. The app also bombarded him with intrusive ads, leading to a compromised gaming experience.



The impact was that John's personal data was at risk, and his device became vulnerable to further malware attacks. The intrusive ads also negatively impacted his device's performance.

Lesson Learned: Only download apps from official app stores to minimize the risk of downloading malicious software. Third-party sources may expose users to fraudulent and harmful applications.

Case Study 3. Digital Payments application

Sanjana and Akash incorporate digital payment applications into their daily routines for the sake of convenience, managing expenses such as house bills and groceries seamlessly through these platforms.

However, their reliance on digital payments takes an unexpected turn when they come across news on TV reporting a server breach in the payment applications they use. This security lapse leads to multiple accounts being compromised, resulting in financial losses for numerous users.

Sanjana experiences a complete loss of funds from her account, whereas Akash, who had wisely set a maximum transaction limit of 5,000 in both his bank account and digital payment application, only incurs a loss of that specified amount. In a subsequent conversation,

Akash elucidates to Sanjana how maintaining a transaction limit acted as a protective measure. This limit thwarted the attacker's ability to extract more than the pre-set amount, demonstrating the importance of prudent financial safeguards in the digital realm.

Case Study 4: "Weak Password Leading to Unauthorized Bank Account Access

Sita: The contribution for the party is ₹1,800. You're attending, right?

Gita: Yes, I'll transfer the money using net-banking.

Sita: I'll do it from your phone. What's your password?

Gita: You already know it! It's my birth date.

Without Gita's knowledge, Sudhir overhears the entire conversation and learns Gita birth date. Exploiting this information, he hacks into her bank account and proceeds to steal money. Concerned about the unauthorized access, Gita reports the incident to the police. The Inspector investigates and identifies Sudhir as the culprit, who confesses to the crime, admitting that he overheard Gita sharing her password.

Reflecting on the incident, Gita acknowledges her mistake in maintaining a weak password and openly sharing it with her friend Sita."

The provided case studies serve as valuable insights, offering a cautionary perspective to enhance your awareness and protect yourself from falling prey to online banking frauds.

Techniques for strong password which are easy to remember

For making unique passwords, create as many passphrases and words as possible (different passwords for different accounts), for example.

- shopping – $h0pp!n9 (S =$, i=!, g=9, o=0)
- october – 0cT0b3r9!
- Social Network – $0c!alNetw0rK
- Windows – w!nD0W$9
- NULinux – 9NuL!NuX

(one more alphabet/number ‘9’ is added as “NULinux” is a 7-letter word)

Mobile App Frauds

Mobile app frauds encompass deceitful activities and unlawful practices occurring within or targeting mobile applications. These deceptive activities pose significant threats to the security, privacy, and financial stability of users. Diverse types of mobile app frauds employ varied tactics to exploit vulnerabilities and mislead users. Examples of such fraudulent activities include:

Types of Mobile App Frauds and Solutions

Fake Apps

Problem: Counterfeit applications impersonate legitimate ones.

Solution: Verify app authenticity, download from official stores, and check user reviews.

Phishing Apps

Problem: Apps designed to trick users into disclosing sensitive information.

Solution: Be cautious of unsolicited links, verify app details, and enable two-factor authentication.

In-App Fraud

Problem: Deceptive practices within legitimate apps.

Solution: Monitor in-app activities, report suspicious transactions, and use trusted app sources.

SMS Phishing (Smishing)

Problem: Fraudulent text messages leading to malicious actions.

Solution: Avoid clicking on unknown links, verify sender identity, and use secure messaging apps.

Subscription Scams

Problem: Users tricked into unauthorized subscriptions.

Solution: Review subscription terms, monitor bank statements, and report discrepancies.

Overlay Attacks

Problem: Malicious apps create overlays to capture user inputs.

Solution: Be cautious with overlay permissions, keep apps updated, and use secure connections.

Credential Stuffing

Problem: Attackers use stolen credentials for unauthorized access.

Solution: Use unique passwords, enable two-factor authentication, and update passwords regularly.

Malicious Software (Malware)

Problem: Harmful software compromises device security.

Solution: Install reputable antivirus software, keep apps updated, and avoid untrusted sources.

Data Leakage

Problem: Apps sharing user data without consent.

Solution: Read privacy policies, limit app permissions, and use privacy-focused settings.

General Tips to Protect Against Online Banking and Mobile App Frauds

- Never share your mobile unlocking PIN or passwords with anyone Keep Software Updated.
- Install reputable antivirus and anti-malware software.
- Verify App Permissions.
- Enable Two-Factor Authentication.
- Educate Yourself.
- Stay informed about common fraud tactics and trends.
- Monitor Account Activity.
- QR codes can be convenient – but they can also be exploited by malicious hackers pointing to scammers payment gateway or website. (Cross check and confirm before any transaction).
- Register your personal phone number and e-mail with your bank and subscribe to notifications. These notifications will quickly alert you on any transaction and the unsuccessful login attempts to your net-banking account.
- Always review transaction alert received on your registered mobile number and reconcile with the amount of your purchase.
- Ensure you use distinct passwords for your social media and banking accounts. Using the same password for both may expose all your accounts to potential risks.
- Always keep a maximum transaction limit for your bank account.
- Secure your applications with strong password and 2-step verification (such as OTP), even for transactions below your maximum transaction limit.
- Uninstall any compromised/malicious application immediately.

By implementing these solutions and adopting proactive security measures, users can significantly reduce the risk of falling victim to various types of mobile app frauds.

In News Cybersecurity, Attacks, Scams

- **70 lakh mobile numbers involved in financial frauds disconnected.**

To check digital frauds, the government has disconnected 70 lakh mobile numbers so far involved in cybercrime or financial frauds, Financial Services Secretary Vivek Joshi said on Tuesday. During the meeting, it was noted that 70 lakh mobile connections involved in cybercrime/ financial frauds reported through digital intelligence platforms have been disconnected so far. About Rs 900 crore of defrauded money has been saved, benefitting 3.5 lakh victims.

- **Gang running online part-time job scam busted; four held for conning of Rs 40 crore.**

305 cases across the country, in which the victims were conned of an estimated Rs 40 crore. During the probe, the cybercrime investigators found that the suspects had operated 30 mule accounts to launder the proceeds of the crime. Mule accounts are those bank accounts that receive money from a third party, which is then transferred to someone else.

- **Ghost' hotels in Puri: Booking hotel room online? Beware of cyber fraudsters**

If you are booking hotels in Puri online, think twice before confirming the booking because cyber fraudsters have become active in this tourist season, setting them yes on gullible people. One such easy target of these fraudsters is Rakesh Haldar, a devotee of Lord Jagannath from West Bengal. Haldar visits Puri every year to have darshan of Lord Jagannath. But this year, he had a bitter experience. While coming to Puri on a train, he was searching for hotels to book a room when he received a WhatsApp message. He also received a video of Hotel Swarna Deep on the New Marine Drive Road in the holy town. He then talked with a person on a number provided and booked a room for five days. He made a payment of Rs 8,000 and Rs

8,830 through PhonePe. When landed in Puri, he realised that he had been taken for a ride as there is no hotel in Puri sharing the name of the hotel he had booked.

- **Delhi Police arrest kingpin who created fake websites of Big Basket, DMart, Blinkit**

Delhi Police has arrested the kingpin of a gang of cyber cheats, which used to create fake websites of e-commerce platforms including Big Basket, DMart, and Blinkit and post lucrative offers to lure unsuspecting buyers and cheat them by stealing their credit card details, an officer said on Wednesday. The accused was identified as Shahrukh Akhtar, who was arrested from Ghaziabad in Uttar Pradesh. According to police, a complaint was lodged with the IFSO (Intelligence Fusion & Strategic Operations) unit, Special Cell. The complainant alleged that while browsing Facebook, they encountered an enticing offer on Big Basket. Consequently, they clicked on the "Shop Now" tab and followed the instructions. Subsequently, an amount of Rs. 98,000 was debited from their credit card.

- **The city cyber-crime sleuths arrested six accused involved in fingerprint cloning.**

The city cyber-crime sleuths arrested six accused involved in fingerprint cloning using rubber fingerprints and Seemandhar machine to illegally withdraw Rs 10 lakh from bank account holders. Prime accused N. Asadharan alias Rupesh, S.Uday Kiran, Md. Iyaz, Ch. Narendra, R. Shiva Krishna and K. Srinu created fingerprints cloning and carried unauthorised transactions in various bank accounts.

- **72-yr-old Pune man downloads ‘APK’ app, loses Rs 13.8 lakh**

A cyber fraudster duped a 72-year-old man in Pune of Rs 13.86 lakh after making him download “APK”, an unverified app, on his cellphone for “updating his PAN card”. The fraudster used an OTP received on the victim’s cellphone to transfer Rs 13.86 lakh from his bank account into another bank account through multiple online transactions.

- **Fake WhatsApp account of officials used to steal money**

By creating fake WhatsApp accounts in the name of district collector Geromic George and PWD secretary Biju K, fraudsters stole money from several people in close contact to them. Through the fake WhatsApp number of the collector, fraudster demanded Rs 50,000 from several people and a few among them sent the money.

- **Fake cops threaten lawyer with drug case, extort Rs 1.9L in Bengaluru**

Cyber criminals have given the FedEx courier scam a new twist. Earlier, the accused would remain invisible and call up the victims and cheat them, posing as Mumbai cybercrime cops and CBI officials. They are now visiting potential victims in police uniforms.

Feeds / Images References

- https://www.pwc.in/industries/financial-services/fintech/dp/combating-fraud-in-the-era-of-digital-payments.html
- https://www.rediff.com/money/report/tech-70-lakh-mobile-numbers-involved-in-financial-frauds-disconnected/20231128.htm
- https://www.deccanherald.com/india/karnataka/bengaluru/gang-running-online-part-time-job-scam-busted-four-held-for-conning-of-rs-40-crore-2788471
- https://odishatv.in/news/odisha/-ghost-hotels-in-puri-booking-hotel-room-online-beware-of-cyber-fraudsters-in-pilgrim-city-219464#google_vignette
- https://www.businessinsider.in/india/news/delhi-police-arrest-kingpin-who-created-fake-websites-of-bigbasket-dmart-blinkit/articleshow/105419735.cms
- https://www.deccanchronicle.com/nation/crime/221123/hyderabad-six-arrested-for-fingerprint-cloning.html
- https://indianexpress.com/article/cities/pune/cyber-fraud-pune-man-apk-app-loses-rs-13-8-lakh-9031379/
- https://www.freepik.com/
- https://cybercrime.gov.in/
- https://www.newindianexpress.com/cities/bengaluru/2023/nov/07/fake-cops-threaten-lawyer-with-drug-case-extort-rs-19l-in-bengaluru-2630736.html

The journey towards cyber safety awareness and data privacy is a continuous commitment to digital well-being. As we navigate the intricate landscapes of the online world, let our collective responsibility be the guiding force. By fostering a culture of awareness, we not only protect ourselves but contribute to the creation of a secure and trustworthy digital environment for everyone.

Remain vigilant, stay protected.

Your cyber safety remains paramount to us.

Continue cultivating responsible online behaviours and staying informed about emerging threats.

We'll be back next month with more tips and updates.

Don't be Quick to Click, think before clicking on links received via email, social media and sms etc.

"Guard your digital castle, lest the wolves of online banking and mobile fraud breach its walls"

THANK YOU