Punjab National Bank

CYBER JAGRITI

Cyber Awareness Handbook

Index

#PNBCyberJagriti

together for a safer cyberspace

Message from
Shri Ashok Chandra
(MD & CEO)

Dear PNBians and our esteemed Customers,

I am delighted to share our vision for a secure and empowering digital banking experience. In today's dynamic digital era, online banking and digital transactions have revolutionized financial management, offering unparalleled convenience and efficiency. This transformation has opened new opportunities for us to serve you better, and we are thrilled to be part of this exciting journey.

At our bank, your trust is our greatest asset. We are dedicated to not only protecting your financial and personal information but also equipping you with the knowledge to thrive in the digital world. It is with great pride that we introduce the PNB Cyber Awareness Handbook, a cornerstone of our commitment to your safety. This initiative is designed to educate and empower you by shedding light on common cyber threats and offering practical, easy-to-follow tips to stay secure.

Within the handbook, you'll discover clear and accessible guidance on navigating risks such as phishing, malware, identity theft, and social engineering scams. Whether you're a digital banking veteran or just beginning your online journey, this guide provides valuable tools to enhance your confidence and security.

Cybersecurity is a collective endeavor, and together, we can create a safer digital banking environment. I warmly invite you to explore this handbook, share its insights with your loved ones, and join us in spreading awareness. Let's embrace the opportunities of digital banking with vigilance and optimism. Stay safe, stay secure, and let's build a brighter financial future together.

Follow these easy steps for better cyber safety and security.

Never Share Your OTP

Dont Click on every Links "Think Before You Click"

Never Share Your Banks and Cards Detail

Use Strong, Unique Passwords

Use Multi-Factor Authentication

Don't use public Wi-Fi for banking

Keep PNB One App updated

General precautions to protect yourself from falling victim to cyber fraud.

Here are some factors that may indicate your phone is being spied on:

Here are key factors indicating your phone may be spied on:

- Unexplained battery drain
- Increased data usage
- Strange behavior or app malfunctions
- Excessive heat
- Odd background noise during calls
- Delayed shutdown or restart
- Unfamiliar apps or icons
- Suspicious text messages or emails
- Overheating when idle

If you notice these signs, consider checking for spyware and securing your phone.

General precautions to protect yourself from falling victim to cyber fraud.

Here are some short precautions for safe internet browsing and avoiding cyber fraud:

Use secure websites
(look for "https://" and a padlock icon).

Avoid public Wi-Fi for sensitive activities; use a VPN if needed.

Keep software updated to protect against security vulnerabilities.

Be cautious with downloads and email attachments from unknown sources.

Adjust privacy settings to limit what others can see online.

What is Cyber Security ?

Introduction to
Cyber Security

Cybersecurity is the protection of computers, smartphones and online information from being stolen, damaged, or attacked by hackers or viruses.

It helps keep your personal data, such as passwords and bank details, safe when you use the internet.

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

HUMANS

The weakest link in cyber security

Humans remain the weakest link in cybersecurity due to their vulnerability to common tactics like phishing and social engineering.

A "2023 report from Verizon" revealed that "36% of data breaches" involved phishing attacks, where individuals are tricked into revealing sensitive information.

Moreover, "81% of hacking-related breaches" were due to stolen or weak passwords, according to the same report. Despite technological advancements, many people still lack proper cybersecurity awareness.

A "2023 study by Proofpoint" found that "83% of organizations" experienced email-based attacks targeting employees, emphasizing that human error continues to be a primary cause of security breaches.

Reason

Why HUMANS are the weakest link in CYBER SECURITY

- Weak passwords are easy for hackers to guess or crack.
- Reused passwords across multiple sites increase vulnerability.
- Social engineering manipulates people into giving away confidential details.
- Clicking on unsafe links from unverified sources can lead to malware infections.
- Disabling security features for convenience weakens system defenses.
- Exposing personal information on social media helps attackers gather details.
- Using outdated software with known vulnerabilities opens the door to attacks.

and many more .....

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

Let us introduce you to some of the cyber frauds happening nowadays.

PHISHING
Attack

Think before You Click.

Don't let them hook you, verify the sender.

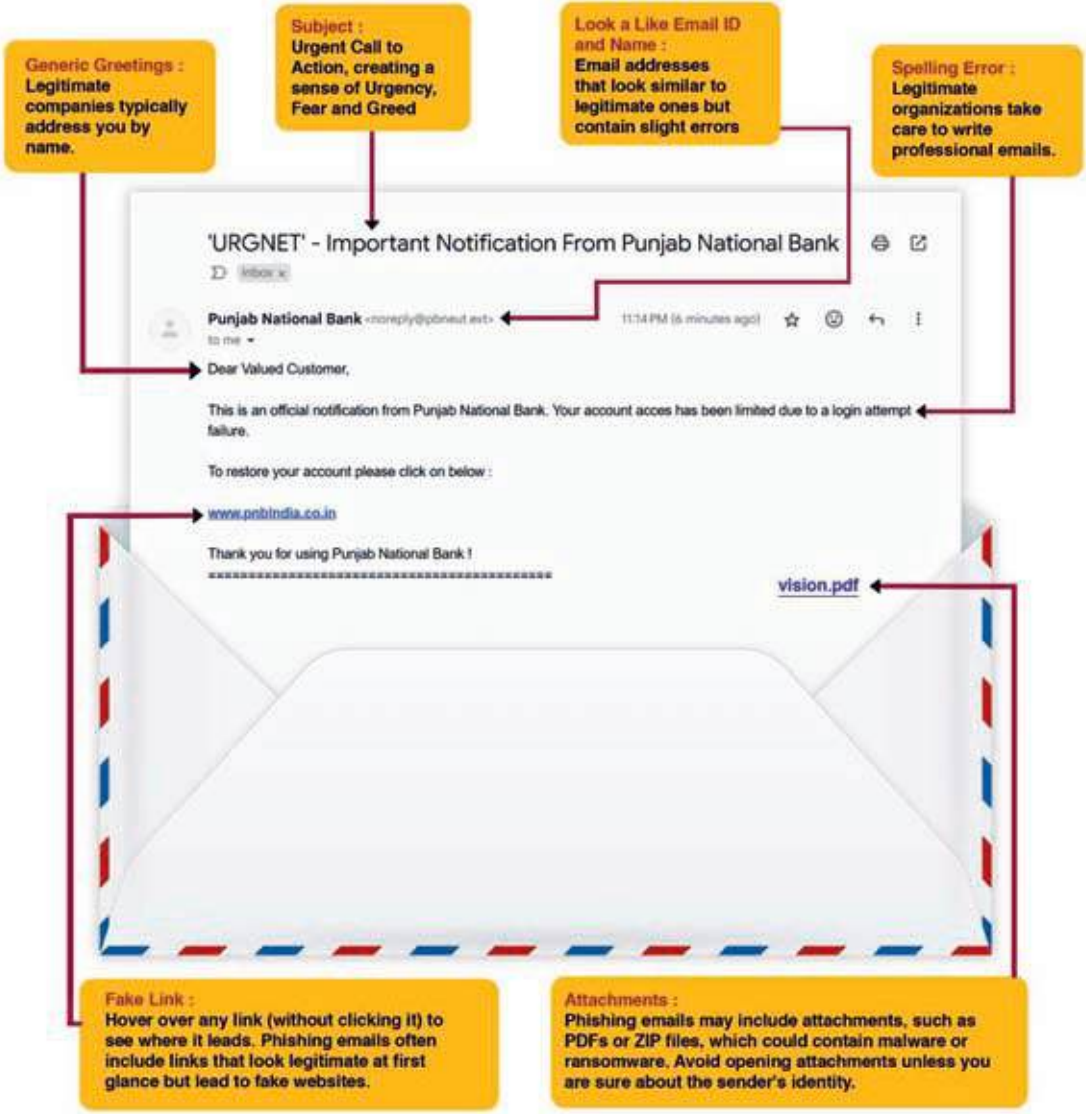
Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

PHISHING ATTACK

You get an email that looks like it's from someone you know or imagine someone pretending to be a trusted source, like your bank, sending you a fake email or text (that's phishing!). They're trying to trick you into giving away your password, credit card number, or other personal info.

How Phishing Email Look Like :



STOP PHISHING

Be cautious with Links, Attachments and requests for personal information

Beware of Urgency

Think Before You Click

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

Phishing Safety Tips

- ✓ Carefully check the URL before clicking on it.
- ✓ Never react to the messages which shows urgency.
- ✓ Look For Generic Greetings: "Dear User," "Hello," "To Whom It May Concern" (instead of a personalized name)
- ✓ Do not trust promotional offers which look “Once in a lifetime opportunity”.
- ✓ Verify the email ids in emails addressed to generic recipients.
- ✓ Look for typing errors (eg., bnak, Acc0unt, ema1l, dep0sit,)
- ✓ Look for poor grammar and unprofessional language.

Safety Tips

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free)
or report @ www.cybercrime.gov.in

UPI FRAUDS

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free)
or report @ www.cybercrime.gov.in

UPI Frauds Scams

UPI fraud typically involves scammers tricking victims into sharing their UPI credentials or OTPs (One-Time Passwords) through phishing calls, fake apps, or fraudulent messages. Once the scammer gains access to the victim's UPI details, they can initiate unauthorized transactions and steal money from the victim's account.

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

UPI Frauds/Scams

Tinku uses UPI in his mobile.

He posted his bicycle online for selling it. He received a call regarding the same.

I saw your advertisement online. I am interested in buying this bicycle.

Sure. When do you want to see the bicycle?

Very soon. But before that I want to send you some token amount so that I don't loose the deal. Can you confirm your UPI ID? I'll send you a QR code in your UPI app. Scan it, and please don't forget to enter the UPI PIN.

Sure. My UPI ID is ****** Send me the QR, I will confirm the receipt of token amount once I scan the QR and enter the UPI PIN.

Tinku lost his money as soon as he scanned the QR and entered UPI PIN.

UPI Fraud Scam - Safety Tips

- ✓ **Never Share: Banks, UPI apps, or government agencies will never ask for your UPI PIN or OTP.**
- ✓ **Strong PIN: Choose a strong, unique UPI PIN that is difficult to guess and change it regularly. Avoid using the same PIN for multiple bank accounts.**
- ✓ **Verify Before Transacting: Double-check the UPI ID and seller credentials before making payments.**
- ✓ **Be Wary of Requests: If you receive a UPI payment request from an unknown source, do not approve it and verify the sender before taking any action.**

Safety Tips

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

VISHING

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

VISHING ATTACK

Vishing, or voice phishing, is a type of social engineering attack where cybercriminals use phone calls or voice messages to trick individuals into revealing sensitive information, such as personal details, financial information, or login credentials. Often impersonating legitimate organizations or authorities, attackers create a sense of urgency or fear to manipulate their victims into compliance. As telecommunication technology continues to evolve, vishing attacks are becoming increasingly sophisticated, making it essential for individuals to remain vigilant.

Vishing

Tinku received a call from a stranger stating that he is calling from XYZ Bank. He informs Tinku that bank has issued him a credit card under a promotional offer.

Hello Sir, I am calling from XYZ Bank. Our bank has issued a credit card under a promotional offer to you as you are a High Net worth Customer of our bank.

I already have one credit card. I don't need another card please. Tell me the process to cancel this new card.

Sir, if you want, I can cancel the card online. It will save your time and efforts. You have to share some information and OTP that you have received on your phone.

Vishing

Tinku: Ok, note down the OTP and cancel the card immediately please.

Tinku received a message on his mobile number informing that his account has been debited by Rs 20000/-.

Tinku tried to call the number from which he received the call but number was not working anymore.

Tinku realized that he should not have shared OTP with a stranger but it was too late now.

Fraudster was able to fool Tinku and extract the confidential information from him through Voice Call.

This is called as Vishing.

Vishing - Safety Tips

- ✓ **Verify Caller Identity – Don't trust caller ID; scammers can spoof numbers.**
- ✓ **Never Share Personal Info – Avoid sharing OTPs, PINs, or bank details over the phone.**
- ✓ **Hang Up & Call Back – If unsure, call the official number from the company's website.**
- ✓ **Avoid Unsolicited Calls – If you didn't request a call, be extra cautious.**
- ✓ **Do Not Press Any Keys – Some scam calls prompt you to press buttons; just hang up.**

Safety Tips

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

SMISHING

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

SMISHING

Smishing, a blend of "SMS" and "phishing," is a fraudulent practice where attackers send deceptive text messages to trick individuals into revealing personal information or downloading malicious software. These messages often impersonate legitimate organizations, enticing recipients with offers, warnings, or urgent requests. Since text messages are typically more immediate and personal than emails, they can elicit a quick, rash response, making users more vulnerable to scams.

Think Before You Tap: Don't Get a Hooked by Smishing!

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free)
or report @ www.cybercrime.gov.in

Smishing

One day, Tinku received a SMS on his mobile number that his account is pending for KYC updation and was advised to click on the link given or call on a given number to update his KYC.

Tinku tried to click on the link provided in the SMS, however, it was not opening. So he decided to call on the number provided in the message.

I have received a message regarding KYC updation, however, I am not able to open the link in the message. Can you help in updating my KYC in the account.

Yes Sir, we are always ready to help our customers. I will update your KYC on call only.

Please share your account details, Aadhar Card, Pan Number, ATM details and ATM PIN so that I can update KYC in the account.

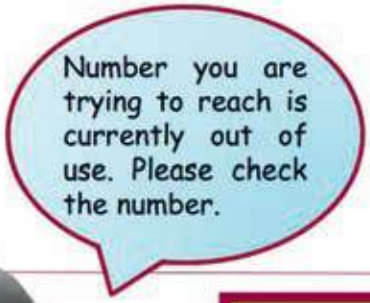
Sir, you have received an authentication code on your phone. You are requested to share that with me.

Smishing

Tinku shared all his confidential details with the caller including the authentication code received by him.

Immediately, Tinku received a message that his account has been debited by Rs 50,000/-.

Tinku tried contacting the number but no one responded.



Tinku realized that sharing information through phone call on the basis of SMS received from an unknown number was a mistake on his part. However, by then, he has lost his hard earned money to a fraudster.

Smishing - Safety Tips

- ✓ **Don't Click on Links – Avoid links in unsolicited texts; they may lead to fake websites.**
- ✓ **Verify the Sender – Check official sources before responding to any SMS.**
- ✓ **Never Share Personal Info – Banks and government agencies never ask for sensitive data via SMS.**
- ✓ **Do Not Respond – Ignoring suspicious messages prevents scammers from targeting you further.**
- ✓ **Use Spam Filters – Enable SMS filtering or blocking on your phone.**
- ✓ **Report and Delete – Report smishing texts to your mobile provider or cybercrime authorities.**

Safety Tips

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

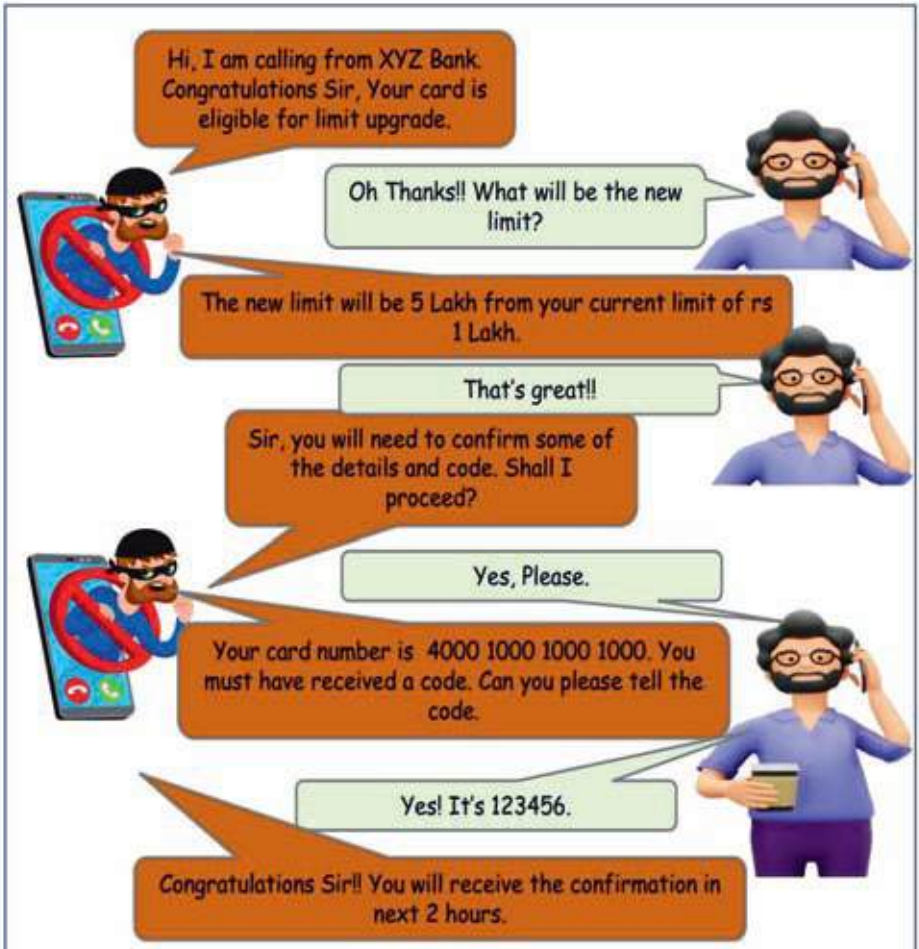
CARD FRAUDS

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

Credit Card Limit Upgrade

Tinku received a call from the Bank.



As soon as Tinku disconnected the call, he received a message about debit of 1.2 Lakh from his credit card. Here, Tinku was defrauded.

Credit Card Activation

Tinku got XYZ Bank's Credit Card.

Tinku believed the fraudster.

As soon as Tinku disconnected the call , he received a message about debit of 1.2 Lakh from his credit card. Here, Tinku was defrauded under the pretext of credit card activation

Card Fraud - Safety Tips

- ✓ **Enable Transaction Alerts – Get instant notifications for all card transactions.**
- ✓ **Never Share Card Details – Avoid sharing CVV, PIN, or OTP with anyone.**
- ✓ **Use Secure Websites – Ensure URLs start with "https://" before entering card details.**
- ✓ **Monitor Statements Regularly – Check your bank statements for unauthorized transactions.**
- ✓ **Set Spending Limits – Restrict daily transaction limits to minimize potential fraud.**
- ✓ **Use Strong Passwords – Enable two-factor authentication (2FA) for online banking.**

Safety Tips

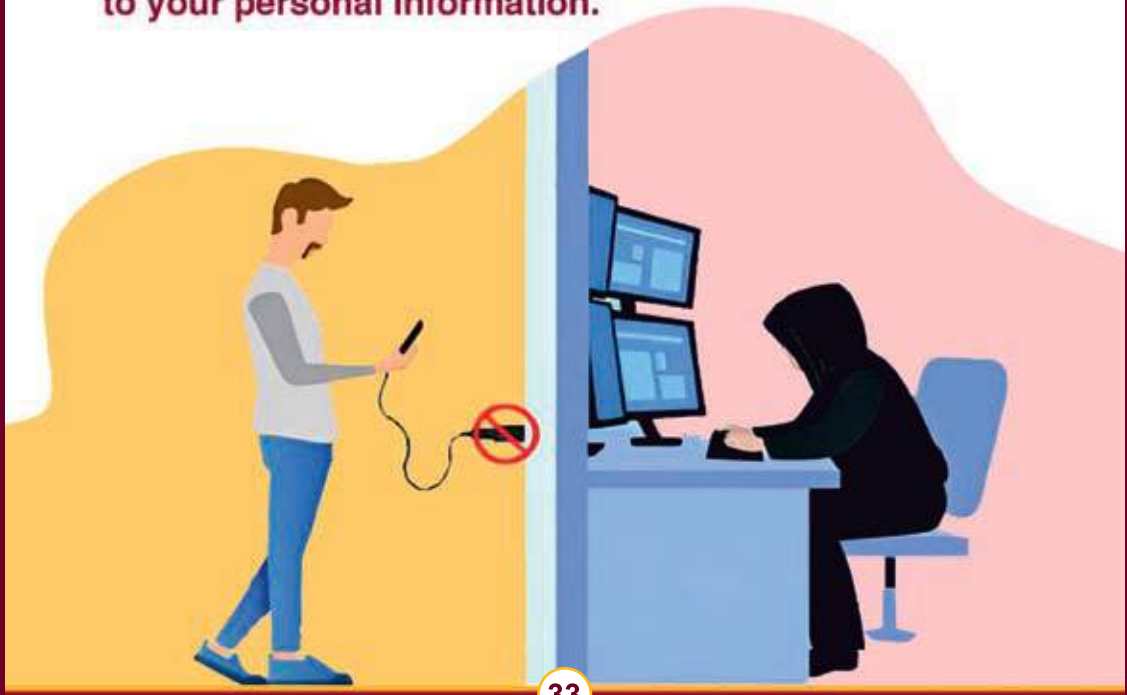
Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

JUICE JACKING

Public USBs: A Hacker's Playground. Charge Safely

Juice Jacking is a security threat that occurs when someone uses public charging stations to steal data from your device while it charges. These stations can be found in places like airports and shopping centres, and they can be tampered with to allow hackers access to your personal information.



Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

JUICE JACKING

Tinku had to leave in emergency. He realized that his phone battery was low.

Tinku : Oh !!! I forgot the charger. Let me find a public charging point.

A fraudster installs charging cable with malware and leaves it as charging point

While charging , malware is injected in Tinku's mobile.

Fraudster got access to his mobile and captured all the details including bank details.

Tinku received messages of unauthorized debit from his accounts.

Juice Jacking - Safety Tips

- ✓ **Avoid Public Charging Stations – Use your own charger and plug into a wall outlet.**
- ✓ **Carry a Power Bank – Keep a portable battery to charge your devices safely.**
- ✓ **Enable Charge-Only Mode – If using public USB ports, select "Charge Only" instead of "Data Transfer."**
- ✓ **Inspect Charging Ports – Avoid tampered or suspicious-looking USB ports.**
- ✓ **Keep Devices Locked While Charging – Prevent unauthorized access during charging.**
- ✓ **Regularly Update Software – Keep your device's OS and security patches up to date.**

Safety Tips

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

KYC SCAM

Beware of KYC expiry scams - verify before you trust.

The KYC (Know Your Customer) expiry scam is a fraudulent scheme where scammers impersonate banks or financial institutions, claiming that your KYC details need to be updated or renewed. They often send messages asking you to provide sensitive information like your bank account number or passwords, leading to identity theft or financial loss.

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.IN

KYC SCAM

Right After this , Tinku got a message that Rs 50,000 have been deducted from his account.

KYC Scam - Safety Tips

- ✓ **Verify the Source – Banks never ask for KYC updates via calls, SMS, or unofficial links.**
- ✓ **Never Share OTP/PIN – Avoid sharing sensitive details with anyone claiming to update KYC.**
- ✓ **Use Official Channels – Update KYC only through your bank's official website, app, or branch.**
- ✓ **Check Email & SMS Authenticity – Look for sender details and grammatical errors in messages.**
- ✓ **Secure Your Bank Account – Enable two-factor authentication (2FA) for online transactions.**
- ✓ **Monitor Account Statements – Regularly check for unauthorized transactions.**

Safety Tips

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

DIGITAL ARREST

Digital arrest fraud is a type of scam where criminals trick individuals into believing they are being investigated or arrested by law enforcement through fake phone calls, emails, or messages. They often demand money to resolve the supposed problem, creating fear and urgency.

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in

DIGITAL ARREST

Tinku received a call from someone claiming to be from a cargo company who told him that there was a parcel for him, which was stuck in Canada.

The parcel contains five passports, a laptop, MDMA drug and clothes.

Its not mine. There is no one I know in Canada.

I will connect you with officials of Cyber-crime, RBI and CBI. You clarify to them regarding the same.

Fraudsters: Hello....the call is on speaker and we are three officers from Cyber-crime, RBI and CBI. If you don't want further troubles, share your aadhar number and Bank Details as your account has been linked with a money laundering case. Amount from your account has been transferred to some missing people's account, and the passport of those missing people is in this parcel for you.

OK, Ok !!!

No no....i am sharing my Bank details please take me out of this trouble, as I have not done anything wrong. This parcel is not mine please believe me.

But your address is written on the parcel with your mobile number. We will now contact you through Video call via zoom and let you know what to do and how to do. You don't get out of your house until we tell you and continue to follow our instructions.

This digital house arrest of Tinku lasted about some 54 hours,during which the accused tricked and forced the panicked Tinku to transfer around Rs. 8.36 lakh in several instalments.

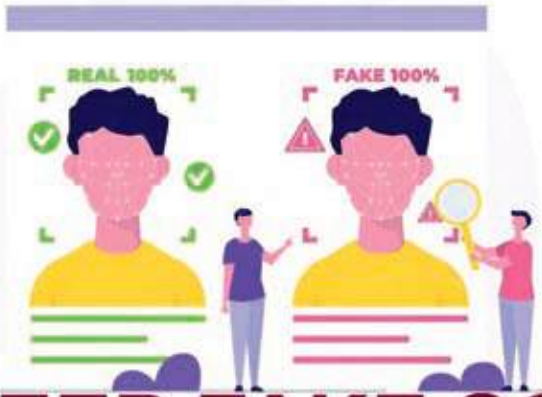
Digital Arrest - Safety Tips

- ✓ **Stay Calm & Don't Panic – Scammers create fear by falsely claiming legal action against you.**
- ✓ **Verify with Authorities – Contact the police or relevant government agencies directly.**
- ✓ **Never Share Personal Info – Avoid giving bank details, Aadhaar, or other sensitive data.**
- ✓ **Do Not Pay Any Money – No genuine authority demands payments over a call or message.**
- ✓ **Block the Fraudulent Number – Prevent further scam attempts by blocking the caller.**

Safety Tips

Cyber and Information Security Division (CISD)

To report cybercrime call 1930 (Toll-Free) or report @ www.cybercrime.gov.in



DEEP FAKE SCAM

What is a Deepfake?

A deepfake is a type of fake video, photo, or audio that uses artificial intelligence (AI) to make it look real. It can change a person's face, voice, or actions in a video to make them appear to say or do things they never actually did.

Why is it Dangerous?

Deepfakes can be used to spread false information.
Criminals may use deepfakes to trick people or steal money.
They can damage someone's reputation or cause confusion.

How to Stay Safe:

Be careful about what you watch and share online.
Don't trust everything you see on social media.
Use trusted news sources to check facts.
If something seems too strange or shocking, it might be a deepfake.

Call Merge Scam

What is the Call Merging Scam?

Cybercriminals are constantly finding new ways to trick UPI users, and one of the latest is the Call Merging Scam.

Here's how it works:

1) A scammer calls you, pretending to be a job recruiter or event organizer.

2) They say they got your number from a mutual friend to gain your trust.

3) Then, they ask you to merge the call with another number — claiming it's their friend or colleague.

4) In reality, the second call is an automated OTP (One-Time Password) call from your bank.

5) By merging the call, the scammer hears the OTP and uses it to access your UPI-linked bank account.

Why is it Dangerous?

1) OTPs are crucial for authorizing UPI payments. If a scammer gets it, they can instantly drain your account.

2) The scam feels believable because it uses familiar scenarios like job offers or event invites.

3) Victims often don't realize they've been tricked until the money is already gone.

Call Merge Scam

How to Protect Yourself from Call Merge Scam

1) To stay safe from call merging scams, follow these tips: Never merge calls with unknown numbers — even if the caller seems friendly or legitimate.

2) Never share OTPs over the phone. Banks will never ask for them.

3) Enable spam call filters on your smartphone to block suspicious calls.

4) Verify unknown callers, especially if they claim to offer jobs or events. Do a background check before engaging.

5) Use secure banking apps and avoid responding to unexpected OTP calls.

6) Report suspicious activity to your bank and call the cybercrime helpline at 1930.

Ransomware

Ransomware is a type of computer virus that locks your files or computer and asks for money to unlock them. Imagine you try to open your photos, documents, or important files—and suddenly, a message pops up saying you must pay money to get them back. That's what ransomware does.

How Does It Happen?

- ✓ It usually comes through emails, fake websites, or infected downloads.
- ✓ Just clicking a bad link or opening a strange file can trigger it.

How to Stay Safe:

- ✓ Don't click on unknown links or attachments.
- ✓ Keep your computer and antivirus software updated.
- ✓ Back up your important files regularly.
- ✓ Use strong passwords and enable two-factor authentication where possible.

Remember:

If you get attacked by ransomware, don't pay the ransom. It doesn't guarantee your files will come back, and it encourages more attacks.

Instead, contact a tech expert or your company's IT team.

Expectations from Everyone for Cybersecurity Hygiene

- ✓ Lock screens when leaving your desk, even for a minute.
- ✓ Use strong, unique passwords and change them periodically.
- ✓ Avoid writing down passwords or sharing them with anyone.
- ✓ Install security updates and patches as soon as they are available.
- ✓ Report suspicious emails, pop-ups, or device behavior immediately.
- ✓ Use only approved software and avoid unauthorized tools/extensions.

Cybersecurity Threats and Their Impact

- ✓ **Phishing can lead to credential theft and financial loss.**
- ✓ **Ransomware may encrypt critical data and demand payment.**
- ✓ **Insider threats can result in data leaks or intentional sabotage.**
- ✓ **Malware/Spyware compromises device and data integrity.**
- ✓ **Data breaches can damage brand reputation and lead to legal penalties.**

Points to Remember for Visitor Movement

- ✓ All visitors must sign in and be accompanied by an authorized staff member.
- ✓ Visitors should wear visible visitor badges at all times.
- ✓ Do not allow visitors into server rooms, data centers, or restricted zones.
- ✓ Report any unidentified or suspicious individuals to security immediately.

In Case of Fire – Fire Protection Measures

- ✓ Know the location of the nearest fire extinguisher and emergency exits.
- ✓ Do not block fire exits or tamper with fire safety equipment.
- ✓ Follow the evacuation plan calmly and assist others if needed.
- ✓ Participate in regular fire drills and training sessions.

Non-Compliance Points to Remember

- ✓ Installing unauthorized software or hardware is strictly prohibited.
- ✓ Using personal USB drives or external devices is not allowed.
- ✓ Sharing confidential data through personal emails or cloud platforms is a violation.
- ✓ Neglecting updates or ignoring security advisories is a compliance failure.

Spyware and Malicious Software

- ✓ Avoid clicking on unknown links or installing unverified apps.
- ✓ Use endpoint protection and anti-malware software.
- ✓ Regularly scan systems for spyware and malicious activity.

Data Modification & Integrity

- ✓ Do not modify or delete data unless authorized and documented.
- ✓ Use version control and audit trails for critical data handling.
- ✓ Ensure encryption is enabled for sensitive or personal data.

Advanced Persistent Threats (APTs)

- ✓ Be cautious of spear-phishing attempts and social engineering.
- ✓ Regularly update systems and monitor for unusual behavior.
- ✓ Use multi-layered security controls (firewall, EDR, DLP, SIEM).
- ✓ Conduct regular threat-hunting exercises and penetration tests.

Email Usage and Password Security

- ✓ Do not open attachments or links from unknown or suspicious sources.
- ✓ Avoid forwarding chain emails or sensitive data without authorization.
- ✓ Use complex passwords with a mix of upper/lowercase, numbers, and symbols.
- ✓ Enable multi-factor authentication wherever possible.
- ✓ Change passwords immediately if you suspect compromise.

Banking Trojans: Many fake APKs are designed as Banking Trojans. Once installed, they monitor the victim's device for banking apps, overlay fake login screens to capture credentials, and gain access to the user's bank account.

SMS hijacking: Some fake APKs can intercept SMS messages, including One-Time Passwords (OTPs) used in two-factor authentication. This allows attackers to complete fraudulent transactions without the user's knowledge.

Remote Access Tools (RATs): Malicious APKs may install a RAT that allows attackers to take control of the victim's phone remotely, enabling them to execute banking transactions or access sensitive information.

Screen overlay attacks: Fake APKs can display overlays over genuine apps, such as payment apps or banking apps. When the user inputs sensitive data, like their PIN or password, the fake APK captures this information.

Credential theft: The fake APK may harvest credentials directly from the device by exploiting stored passwords, autofill information, or phishing attacks within the app.

Fake investment or payment apps: Attackers sometimes create entire fake apps for investment schemes or payment services that appear legitimate. Users are tricked into entering their financial details or making payments, which are directly stolen by the fraudsters.

Social Engineering Attacks: Example: You receive an email that says, "Congratulations! You have won a prize of ₹10,000! To claim your reward, click here: [fake link]."

What Happens: The link directs you to a form asking for personal details like your bank account number, IFSC code, and other sensitive information. The fraudster uses this information for identity theft and financial fraud.

Tech. Knowledge

Do's

- ✓ Do verify any communication regarding your PNB account by directly contacting the bank through official channels.
- ✓ Do download only from legitimate app stores and check user reviews before installing any app.
- ✓ Do ensure our devices are updated regularly with the latest security patches.
- ✓ Do use a strong, unique password for your PNB online Banking
- ✓ Do report any suspicious emails, SMS, or transactions to PNB's fraud helpline immediately.

Don'ts

- × Don't click on links in unsolicited emails, SMS, or social media messages, even if they claim to be from PNB or offer something exciting.
- × Don't share your banking credentials (password, PIN, OTP) with anyone, even if they claim to be a bank employee.
- × Don't install apps from unknown or unverified sources.
- × Don't ignore warnings from your phone or security software about suspicious apps or websites.

Message from

Ashwini Kumar Pandey
(Group CISO)

Dear Stakeholders,

The protection of sensitive financial and personal data has become a major concern in this era marked by rapid digital transformation. As cyber threats grow in complexity and frequency, cybersecurity is a shared responsibility that involves systems, processes, and people.

At our bank, we have adopted a multi-layered security approach that combines advanced technology, rigorous policies, and constant monitoring to safeguard our infrastructure and customer data. However, technology alone is not enough. The human aspect is of major concern as well. Cybercriminals often exploit human vulnerabilities through social engineering, phishing and fraudulent schemes. This is why it is important to create user awareness as a critical element of defense against cyber frauds.

This booklet has been developed with the objective of educating and empowering our valued customers with the knowledge to recognize potential cyber threats and take proactive steps to protect yourselves. I urge you to take the time to familiarize yourself with the contents of this booklet, implement the best practices outlined, and stay alert in the digital world

Cybersecurity is more than a one-time effort; It is a continuous journey. Let us move forward on this journey together-secure, informed, and resilient.

To report cybercrime,

call at

1930

(Toll-Free)

or report @

www.cybercrime.gov.in

Cyber and Information Security Division (CISD)