Punjab National Bank (PNB) Advisory: Protect Yourself from Cyber Threats - Unsolicited Apps and Links

Cybersecurity threats continue to rise, with criminals constantly seeking new ways to deceive users through unsolicited links and apps. Punjab National Bank (PNB) is committed to helping clients stay protected against these threats by raising awareness on how cybercriminals operate and how you can safeguard your information.

Modus Operandi of Cybercriminals

Cybercriminals use various techniques to lure users into clicking malicious links or downloading harmful apps. Here's how these attacks typically unfold:

1. **Malicious/ Fake Apps**:

• **Example**: You get an exciting offer via a WhatsApp message:
"Install this app to get 50% off on all your purchases this Diwali! Click here to download now: [malicious link]."

• **What Happens**: Clicking the link installs a seemingly harmless app, but behind the scenes, the app has permissions to access your messages, contacts, and even sensitive data such as stored passwords or banking information. Some apps also record your keystrokes to capture passwords and PINs. **Always Download applications from Google Play Store or Apple App Store.**

Fake APKs are malicious apps disguised as legitimate apps and shared through various distribution methods, with the goal of siphoning money or stealing sensitive information from unsuspecting users. Here's how fake APKs are commonly received, shared, and used for financial fraud:

```
#   barcode-dbg
#   kbarcode
#   libbarcode-code128-perl
#   libbarcode-zbar-perl
#   libgd-barcode-perl
#   libpdf-reuse-barcode-perl
#   libpostscriptbarcode
#   php-image-barcode
metal@metal /tmp/barcodes $ barcode -b "This is my first barcode" -o first.ps
metal@metal /tmp/barcodes $ display first.ps
metal@metal /tmp/barcodes $ barcode --help
barcode: Options:
  -i <arg>     input file (strings to encode), default is stdin
  -o <arg>     output file, default is stdout
  -b <arg>     string to encode (use input file if missing)
  -e <arg>     encoding type (default is best fit for first string)
  -u <arg>     unit ("mm", "in", ...) used to decode -g, -t, -p
  -g <arg>     geometry on the page: [<wid>x<hei>][+<margin>+<margin>]
  -t <arg>     table geometry: <cols>x<lines>[+<margin>+<margin>]
  -m <arg>     internal margin for each item in a table: <xm>[,<ym>]
```

Distribution Methods of Fake Apps

- Third-party app stores: Fake APKs are often shared on unofficial app stores, which are less secure than official platforms like Google Play. These third-party stores may host modified or fake versions of popular apps.
- Phishing links: Cybercriminals send links to fake APKs via phishing emails, SMS, or social media messages. These links often impersonate legitimate businesses or popular apps, prompting users to download malware-laden APKs.
- Social engineering: Attackers create fake websites mimicking genuine services (like banking apps or popular e-commerce platforms), tricking users into downloading the fraudulent APKs.
- Instant messaging apps: Fake APKs can be shared directly through WhatsApp, Telegram, or similar platforms. Users receive messages claiming that the APK is a useful app or a required update.

Techniques Used to Siphon Money

- 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.

How Money is Siphoned

- Direct access to bank accounts: With stolen credentials, attackers can log into the victim's bank account and initiate unauthorized transfers or payments.
- Mobile wallets and payment gateways: Fake APKs may target mobile wallet apps (e.g., Paytm, Google Pay) to make fraudulent transactions or steal funds stored within these accounts.
- Fraudulent in-app purchases: Attackers may make unauthorized in-app purchases or subscriptions using the victim's linked payment methods.
- SIM swapping and identity theft: Some fake APKs work in conjunction with SIM swap scams, where the attacker gains control of the victim's phone number to bypass OTP-based security.

Preventive Measures

- Download only from official stores: Users should download apps only from trusted sources like the Google Play Store.
- Verify app authenticity: Before installing any app, users should verify the developer's name, app reviews, and permissions requested.
- Use mobile security solutions: Installing a reliable mobile antivirus or security app can help detect and block fake APKs.
- Avoid clicking on suspicious links: Users should be cautious of unsolicited emails, SMS messages, or social media links, especially those promising apps or updates.
- Enable 2FA via hardware tokens or apps: Using two-factor authentication methods that do not rely on SMS (e.g., hardware tokens or authenticator apps) can help prevent attackers from using intercepted OTPs.

2.**Phishing Emails and SMS**:

- **Example**: You receive an SMS that reads:

"Dear PNB Customer, your account has been temporarily blocked due to unusual activity. Please click the link to verify your account: [fake link]. Failure to verify will result in account suspension."

- **What Happens**: The link takes you to a fake website that looks almost identical to PNB's official site. Once you enter your credentials (username, password, and even OTP), the attackers steal this information and use it to drain your account or commit fraud.

3. **Fake Customer Support Calls or Emails**:

- **Example**: You get a call from someone claiming to be a PNB representative. They tell you there is a problem with your account, and they need your account number, password, or OTP to resolve it.
- **What Happens**: The caller is a fraudster. Once they have your information, they can gain access to your account, transfer money, or commit identity theft.

4. **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.

Best Practices to Stay Safe

PNB encourages you to adopt the following cybersecurity practices to protect yourself from becoming a victim of online fraud.

1. **Download Apps from Trusted Sources**:
- Only download apps from official stores like the **Google Play Store** or **Apple App Store**. Avoid downloading apps through links shared via SMS, email, or social media, as these could be laced with malware.
- **Example**: A genuine PNB app will only be available on official app stores. If you receive an offer to download an app via a link in a message, it's best to ignore it.

2.**Think Before You Click**:
- Always be suspicious of unexpected emails or SMS, especially those containing links or attachments. Even if the message seems urgent or official, **verify its authenticity** before taking any action.
- **Example**: If you receive a message about your account being blocked, don't click on any links. Instead, call PNB customer service directly using the official number on our website to verify the message.

3. **Verify Suspicious Communications**:
- If you receive a message asking you to act quickly to resolve an account issue, don't panic. Visit PNB's official website or call customer care directly to verify the information.
- **Example**: Instead of clicking on a link in a message that claims your account has been compromised, log in to your PNB account from the official website or app and check for any alerts there.

4. **Check URLs Carefully**:
- Before entering sensitive information on a website, double-check the URL. Ensure that it starts with **"https"** and has the correct domain name (**pnbindia.in**). Cybercriminals often create fake websites that look almost identical to legitimate ones, with small changes in the URL (e.g., "pnblndia.in" instead of "pnbindia.in").
- **Example**: A message with a link like "pnbcustomerverify.com" is not legitimate. Always verify the domain and ensure it belongs to PNB before entering any details.

5. **Secure Your Devices**:
- Regularly update your phone's operating system and apps to protect against vulnerabilities. Install security software to detect malware and prevent harmful apps from accessing your data.

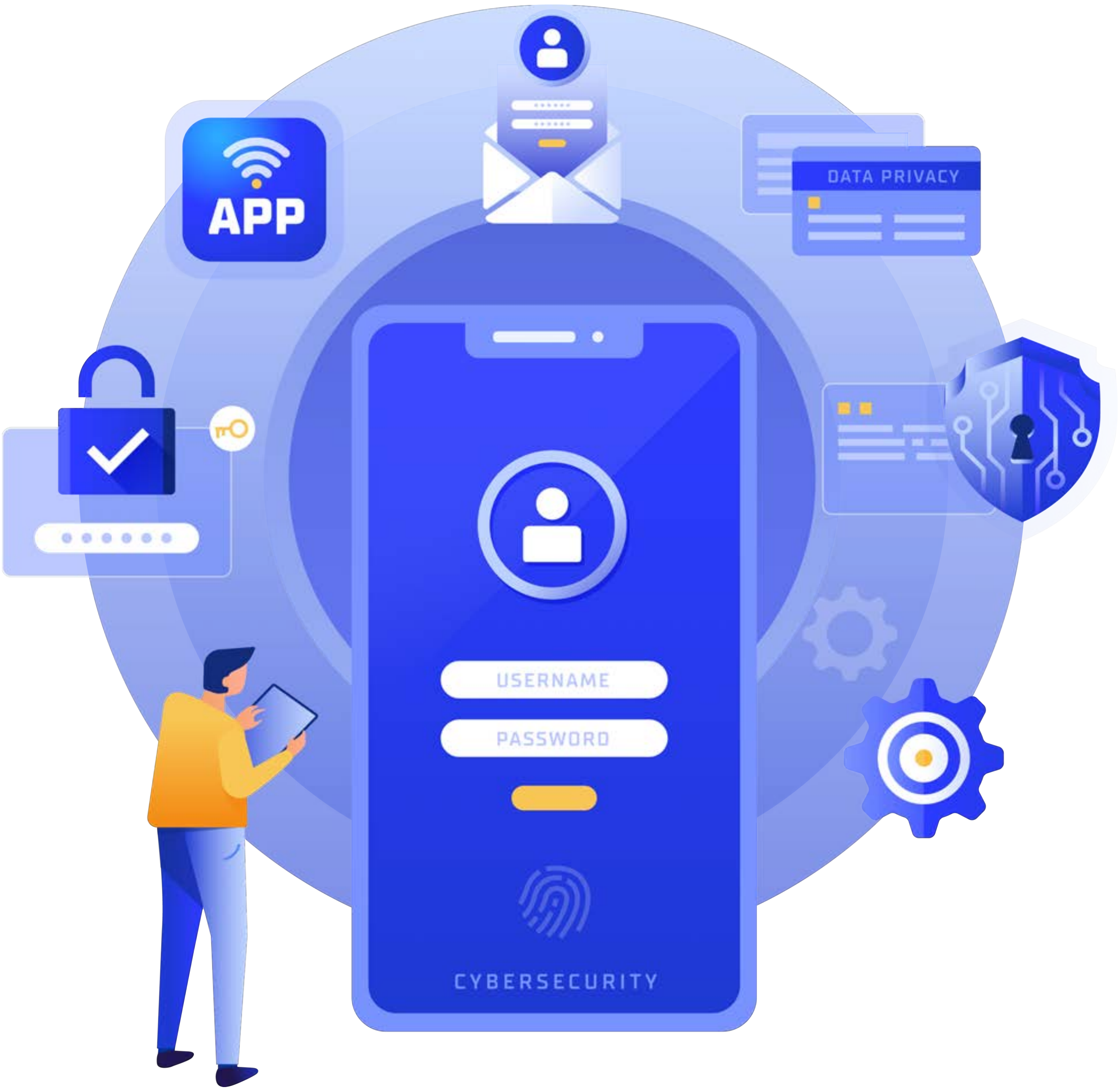
6. **Monitor Your Accounts Regularly**:
- Frequently check your bank statements and online account activity for any suspicious transactions. Report any unauthorized activity to PNB immediately.

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** your 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.
- **Don’t trust** messages that create a sense of urgency, such as those claiming you need to act immediately to avoid account suspension or loss of funds.



Cautions

- **Beware of Unverified Sources**: Cybercriminals often lure users through social media ads or links that look legitimate but direct you to unsafe apps or websites.

Example: A festive sale offer sent via WhatsApp may seem appealing, but it could be a trap to install malware on your phone.

- **Avoid Sharing Sensitive Information**: No genuine institution, including PNB, will ask for your password, OTP, or other sensitive information via email, phone call, or SMS.

Example: If someone claiming to be from PNB asks for your OTP over the phone, it is a scam. Hang up immediately and report the incident to PNB.

- **Watch Out for Social Engineering**: Attackers may try to manipulate your emotions by creating panic (e.g., claiming your account has been hacked) or excitement (e.g., offering rewards for clicking a link). Always take a moment to verify the authenticity of such claims before acting.

PNB Contact Information

If you suspect that you've been targeted by a cyberattack or have encountered a suspicious message, immediately contact Punjab National Bank:

- **Helpline**: 1800 180 2222 / 1800 103 2222
- **Email**: care@pnb.co.in
- **Website**: www.pnbindia.in

Stay Vigilant, Stay Secure with PNB Cybersecurity Awareness

pnb