Important Security Alert: Beware of Malicious Apps Targeting Financial Users and Fraudsters exploiting compromised websites for public deception

We would like to alert you about a large-scale scam campaign targeting users of Indian financial organizations through malicious Google Play Store download pages. This scam attempts to steal sensitive user information by tricking users into downloading fake applications that appear to be legitimate.

What You Need to Know:

- Threat actors are creating fake Play Store websites that mimic the official platform to deceive users.
- These malicious applications (APKs) are designed to steal banking credentials, monitor keystrokes, extract contact lists, and track clipboard contents.
- The malware specifically targets Android devices running versions between 7.0 (SDK 24) and 13.0 (SDK 33).

How to Protect Yourself:

1. **Download Apps Safely:**
    - Only download apps from trusted sources such as the official Google Play Store or your device manufacturer's app store.
    - Avoid side-loading apps by ensuring the "Untrusted Sources" setting remains disabled.
2. **Review Apps Carefully:**
    - Always verify app details, user reviews, and download statistics before installing.
    - Check the "ADDITIONAL INFORMATION" section for suspicious details.
3. **Check Permissions:**
    - Only grant app permissions that are relevant to the app's functionality.
4. **Stay Updated:**
    - Regularly install Android updates and security patches from your device manufacturer.
5. **Exercise Caution Online:**
    - Avoid clicking on untrusted links or suspicious messages received via SMS, email, or social media.
6. **Be Alert for Suspicious Numbers:**
    - Scammers may use email-to-text services or random numbers to mask their identity.
    - Bank-related SMS messages typically display a sender ID rather than a phone number.
7. **Examine Links Carefully:**
    - Only click on URLs that clearly show the organization's website domain. If unsure, visit the website directly via search engines.
8. **Strengthen Your Security:**
    - Install and maintain updated antivirus and anti-spyware software.
    - Use safe browsing and filtering tools to enhance security.

9. **Check for Secure Websites:**
    - Look for a valid encryption certificate (green lock icon) in your browser's address bar before entering sensitive information.
10. **Stay Informed:**
    - Participate in cybersecurity awareness programs and stay informed about online threats.
11. **Report Suspicious Activity:**
    - If you notice any unusual activity in your account, immediately contact your bank for prompt action.

For any incidents related to this campaign, we urge you to report them immediately to CERT-In at **incident@cert-in.org.in**. and mail us at cyberincident@njgroup.in or contact us at 0261-4025836.

Furthermore, please be informed of our official website https://www.njwealth.in. We strongly urge you to remain cautious and verify all information exclusively through our official channels before engaging in any transactions. The list of our official channels and handles are available on https://www.njwealth.in.

Your security is our top priority, and we are committed to providing you with the best practices to safeguard your personal and financial information.

Stay Safe, Stay Secured.