Article > Enhancing Your Financial Wellness: The Seamless Customer Experience of Savings Accounts with Added Benefits

Online security best practices for banking transactions

Banks are major targets for cyberattacks, making them vulnerable to security breaches and exploits.

By Ratan Jyoti, Chief Information Security Officer (CISO), Ujjivan Small Finance Bank | 9th Feb, 2024

Given the vast number of customers banks serve today and the sensitive and personal data they hold, safeguarding against cyber threats has become a principal concern for the banks. The emerging cyber threats and the interconnected world make things difficult, as in today's connected world, digital security threats pose a significant risk to individuals and businesses alike. Malicious actors leverage various methods to compromise online security, with some of the most common threats being malware, phishing, and ransomware. Recent trends in Digital fraud include QR code fraud, Phishing/SMShing/Vishing, and Social Engineering. The reason behind getting duped with this modus operandi is humans falling prey to the fraudsters' smooth talk.

Nowadays, banks are focusing on providing such security services to consumers to safeguard their interest vested in banking and financial institutions. Best practices while using different digital payment channels which an individual may consider while using any of them is as follows: -

a) Always prefer bank-provided UPI application channels. If your bank does not have an integrated UPI application, please download authorised application from authorized app stores.

b) Enable Internet Banking with multi-factor authentication. If your Bank provides MAC (Media Access Control Address) binding, you may opt for it.

c) Mobile Banking

- Do not install Apps from third party app-stores
- Install only the apps that are needed
- App rights management (Provide rights on need basis/relevant to the apps purpose only)
- Always enable multi-factor authentication MFA for making transactions if provided by the Bank

d) AEPS

- Lock biometric information and AEPS default settings through m-Aadhar
- Don't share your Aadhar number with anyone.
- Craft robust passwords, regularly update them, and consider using a password manager for added convenience.
- Regular update your device software to benefit from the latest security patches.

e) Safe Browsing Habits: Verify website authenticity, be cautious of unsolicited emails, and avoid clicking suspicious links. Browser Hygiene: -

- Autofill / Credential Storage
- Safe Extensions
- Always use Https://url
- Always use incognito mode while making transactions.
- Regular Updates
- Privacy focused Browsers
- Disabling lower versions of SSL

f) Social Media Awareness: Exercise caution when sharing personal information online to minimize the risk of identity theft.

g) Monitoring Accounts: Regularly review your financial statements and credit reports to detect any unusual activity promptly.

h) Shredding Documents: Dispose of sensitive physical documents securely to prevent identity theft.

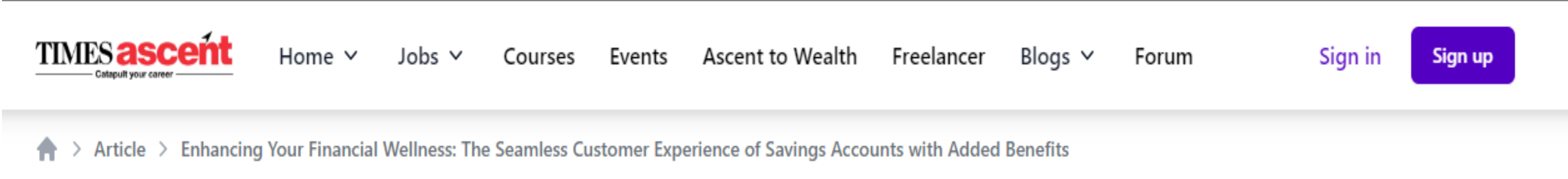
i) Internet of Things (IoT): Be mindful of security considerations for connected devices to avoid vulnerabilities in your network.

j) Unsecure Wi-fi: - Never connect to unsecured Wi-fi, it may be freely available but can cost you more than a network recharge.

k) Reporting Cyber Crimes: Familiarize yourself with procedures for reporting cyber incidents to relevant authorities.

Banks may use the new generation technologies like Artificial Intelligence (AI) based Anti-Fraud and anomaly detection to prevent frauds. Data Mining and AI are two such powerful tools. Machine learning for data driven fraud detection can be very useful wherein model's accuracy and self-learning can improve over time. Conversational AI can be used to detect transactional behaviour anomaly. Whereas Voice AI solution can prevent voice-based scams prevalent today, the voice biometrics can be used to authenticate the right the user.

In an era dominated by technology, ensuring the security of our digital lives has become more critical than ever. From personal data to financial transactions, the online realm is teeming with potential



threats. Digital security is the bedrock of a safe online experience. Understanding these digital security threats is the first step towards fortifying your online presence.

In conclusion, proactively implementing these measures will significantly bolster your digital security. Stay vigilant, stay informed and stay secure in the vast digital landscape.

---END--

Link - https://timesascent.com/articles/online-security-best-practices-for-banking-transactions/158312