The Reserve Bank of India Mandate: an opportunity to fight costly ATM attacks

ATM attacks cost more than just money. Banks that suffer high-profile breaches often struggle to shake off the perception that customer money isn't safe with them, and that can lead to customers returning to holding their money in cash at home rather than in a bank. The RBI mandate is an opportunity to protectively address potential security vulnerabilities at the self-service channel to prevent an attack before one occurs. This helps protect not only the bank's reputation but the customer's peace of mind.

Biggest breach.

In the biggest breach of the year[1], hackers skimmed customer data and used it to steal ₹490 million over three days in August 2018.

Skimming – a device applied to the ATM by criminals to capture PIN and card data which can be used to create counterfeit cards for use in stores, ATMs and online.

Tiniest ATM thief.

Sometimes the thief is the culprit you least suspect. In June 2018, rats got inside an ATM in Tinsukia and ate ₹1.2 Million.[2] When it comes to security, you really have to make sure you've got everything covered.

76 cases in 8 days.

Over 8 days in July 2018, more than 76 cases of ATM fraud, mostly from skimming, were filed in Kolkata. The thefts cost customers up to ₹50,000 each.[3]

WHILE IT'S IMPORTANT FOR BANKS TO BE VIGILANT ABOUT THE SECURITY OF THEIR HARDWARE AND SOFTWARE, IT'S EQUALLY IMPORTANT TO EDUCATE CUSTOMERS ABOUT HOW THEY CAN KEEP THEIR BANK ACCOUNTS SAFE.

Keep your PIN secret.

Never use an ATM if someone is loitering nearby. Customers should never give their PIN or OTP number to anyone – even family members, and never keep a written record of it in the same place as your card. In June 2018 a woman in Dhayari lost ₹18,000 after a pickpocket stole her ATM card – which she had written her PIN number on.[4]

Get mobile alerts.

If your bank provides alerts to your mobile phone, use it to let you know when money is withdrawn at ATMs or when your card is used in a shop. This will alert you to suspicious activity as soon as it happens, and helps you get in touch with your bank to stop it faster.

Check the ATM for skimmers.

Look for anything unexpected or out of place at the ATM, especially around the card slot. Wiggle the plastic slot casing to make sure it's firmly attached. If something doesn't look and feel like it matches the rest of the ATM, report this immediately and find another one to use. Use mobile pre-staging to take the plastic card out of the ATM interaction altogether.

Mobile pre-staging – using a mobile banking app, consumers can request an ATM withdrawal. Instead of using a card and PIN, the consumer uses their phone to unlock the transaction at the ATM and get their cash.

IF YOU'D LIKE TO LEARN MORE ABOUT ATM SECURITY OR TO DISCUSS HOW NCR CAN HELP YOU MAKE THE MOST OF THE RBI OPPORTUNITY, EMAIL US AT: RBI.MANDATE@NCR.COM AND WE'LL GET RIGHT BACK TO YOU.

Sources

[1]https://csecybsec.com/cse-news/cosmos-bank-hackers-stole-rs-94-crore-13-5-million-in-just-in-2-days/
[2]https://www.reuters.com/article/us-india-bank-rat/rat-breaches-bank-atm-in-india-eats-18000-worth-of-cash-idUSKBN1JH31U
[3]https://indianexpress.com/article/cities/kolkata/kolkata-in-8-days-76-cases-of-atm-skimming-5287502/
[4]https://timesofindia.indiatimes.com/city/pune/pin-written-on-atm-card-cover-costs-woman-rs18k/articleshow/65155467.cms