NUSOURCE

Top 10 Self-Service Security Threats

(& How to Avoid Them)

The financial services industry is experiencing a steady growth of unprecedented threats. The complexity and variability of these threats demand a security solution that is not only comprehensive but also adaptable to the ever-changing landscape of financial crime. Statistics share a sobering fact: no aspect of your institution's security is immune. However, your FI does not have to be a victim.

NuSource is the trusted partner to protect your FI.

Our strategy extends beyond traditional surveillance, incorporating real-time and remote monitoring, intelligent analytics, cyber security, and proactive threat detection. We understand the immense responsibility of safeguarding your customers' physical and economic well-being and we have the tools, expertise and reputation to stop criminals in their tracks.

This communication is both informative and crucial. It is meant to educate you about the latest threats targeting financial institutions, but also to inspire and empower you to take proactive action. It is critical to be informed of potential vulnerabilities and strengthen your defenses against unnecessary risk.

1. **Tow & Hook**
2. **Cash-Out Attack**
3. **Jack Potting**
4. **Man-in-the-Middle**
5. **Black Box Attack**
6. **Skimming/Shimming**
7. **Shoulder Surfing**
8. **Glue and Tap Scam**
9. **Service Call Exploitation**
10. **Phishing and Vishing**

Call for more info **952-942-9191**

9749 Hamilton Road
Eden Prairie, MN 55344

nusource.com

sales@nusource.com

Here's a breakdown of the 10 most common attacks and how your FI can fight back:

Physical Attacks & Theft Devices:

Tow & Hook: A truck aligns to the ATM in a "T" formation. The thief attaches a chain and hook to the ATM and uses the truck's strength to rip off the front and steal interior currency.

Cash-Out Attack: Criminals remove the ATM outer shell, hand off the hard drive to a waiting coder who installs an executable code, and sets a command for the ATM to dispense all internal currency as soon as it is replaced.

Jack Potting: Similar to Cash-Out, the criminal uses other types of physical access to an ATM and installs malware on the machine via an open port (USB or Ethernet). The sophisticated malware scans and then takes advantage of the ATM's software vulnerabilities and commands it to dispense all the cash in the internal cassettes. This type of theft is not tied to a card or any specific account but to all the cash within the ATM and can be devastating to a financial institution.

Man-in-the-Middle (MITM): Another form of Jack Potting, attackers place a device between the ATM and the host computer to intercept, eavesdrop, modify, or impersonate communication for fraudulent purposes without need to access the ATM casing. Often accessed via the cables that are connected to the bank and larger services this is a significant risk.

Black Box Attack: Black Box devices are small, portable electronic devices often built around a single-board computer that exploit security weaknesses. The black box either connects directly to the cash dispenser, bypassing controls and stealing money, or takes advantage of software flaws to gain control of the entire ATM. These devices are becoming readily available on the black market, and rising in use by organized crime rings which is raising concerns that these attacks could become more widespread. Their stealthy nature makes them difficult to detect in real-time, allowing criminals to steal very large sums quickly.

There has been a 71% year-over-year increase in cyberattacks that used stolen or compromised credentials.

Card & Data Stealing Threats:

Skimming/Shimming (also known as a Deep Insert Skimming): Criminals install a fake card reader or wafer-thin device onto or within the ATMs/ITMs. Difficult to detect, the device steals your card's data directly from the magnetic stripe. However, although it steals card data it cannot access the PIN. Criminals often use hidden cameras on the ATM fascia to capture the PIN as users enter it.

Preplanned Street Theft:

Shoulder Surfing: Nefarious actors use stealthy methods to steal PIN data from unsuspecting ATM users. They may follow the user and steal the card at another location (assault, purse snatching, pickpocketing or even home invasion), and then return to the ATM to empty the user's accounts. Then there is a rise in ATM muggings. Rather than follow the user to steal the card at another location, the bad actor threatens the user while using the ATM and forces them to access and drain accounts.

Glue and Tap Scam: This involves criminals tampering with the card reader by placing something inside it that blocks card insertion. The criminal then acts as a helpful bystander who suggests using the tap-to-pay option. Since tapping often bypasses the log-out function, fraudsters can steal money from the active session once the customer leaves the vicinity.

Service Call Exploitation: In some cases, thieves might create fake service requests to lure technicians to a specific ATM. This could be a way to distract them or create an opportunity for a robbery.

Phishing and Vishing: Fraudsters might contact an email list of victims and pretend to be a legitimate vendor. They request sensitive information under the guise of a security check. Sometimes, the more sophisticated thieves will employ an email phishing scheme targeted to a specific user they have researched. Referred to as "Spear Phishing", the perpetrator curates a custom and very realistic "corporate" email that encourages the user to enter personal data in response to a recent transaction or activity. He or she then withdraws from the user accounts before the theft is recognized as illegitimate.

20 ATM/ITM Security Solutions to Protect Your FI

For financial institutions to confidently face the relentless assault on physical security and data integrity, NuSource proudly offers a comprehensive and proactive security strategy. This strategy tackles threats at every level, ensuring the safety of your assets and your customers' information.

Prevent Unauthorized Access:

Reinforce ATM Enclosures: Upgrade ATM exteriors with high-strength, tamper-resistant materials like reinforced steel. This deters tow & hook attempts and "ram raids," where criminals use vehicles to force entry.

Protective Bollards: Install sturdy bollards or barriers around ATMs/ITMs to prevent physical attacks and create a buffer zone for security cameras.

Remote Monitoring: IoT sensors monitor temperature, humidity, and tampering.

Regular Inspections: Maintain a consistent and rigorous maintenance schedule to ensure that ATMs are in top condition and have not been compromised.

Secure Locations: Install and ensure ATMs/ITMs are in well-lit, high-traffic areas, or consider placing them inside bank branches or other secure locations.

High-Security Access: Implement robust access control systems. Utilize multi-factor authentication and tamper-evident seals on access points to ensure only authorized personnel can access ATM/ITM maintenance panels and cash cassettes.

Cash Cassette Security: In addition to a robust container and locking system, install anti-theft dye packs that stain stolen cash to deter theft further. Implement cash replenishment schedules to minimize risk.

Unwavering Surveillance: Employ a comprehensive video surveillance system featuring high-resolution cameras with strategic placement to achieve complete coverage of ATMs/ITMs inside and outside the enclosure.

Multi-Layered Alarm Systems: Deploy robust alarm systems with loud sirens, flashing lights, and even smoke canisters to deter potential criminals and alert authorities instantly.

Combating Card & Data Theft:

EMV Chip Technology: Encourage or require customer adoption of EMV chip cards, which offer significantly more robust security than traditional magnetic stripe cards.

Anti-Skimming Devices: Deploy physical anti-skimming devices on card readers. These specialized attachments act as barriers, making it impossible for criminals to install skimming equipment that steals card data.

PIN Pad Covers: Provide PIN pad covers for customers to shield their PIN entries from hidden cameras strategically placed by criminals.

NUSOURCE

End-to-end Hard Drive Encryption: Encryption protects data transmitted between ATMs /ITMs, the financial institution's network (SSL/TLS 1.2) and the hard drive. Also be certain to include cyber security to prevent unauthorized access to software.

Communication Encryption: Implement robust data encryption protocols like TLS 1.2 on all ATMs/ITMs. This safeguards sensitive financial data communicated between ATMs/ITMs and your network from unauthorized access.

Network Security: Fortify your network infrastructure with advanced security solutions. Utilize firewalls to filter incoming and outgoing traffic and implement intrusion early detection systems to identify and prevent cyber attacks targeting your ATMs/ITMs.

Real-Time Video Alerts: Integrate real-time video monitoring systems that leverage advanced analytics and machine learning. These systems continuously monitor transactions and flag suspicious activity based on predefined parameters, allowing immediate intervention.

Software Updates: Maintain a consistent and rigorous software update schedule for all devices and systems associated with your ATMs. This ensures your network remains patched against the latest vulnerabilities cyber criminals exploit.

Cash Reconciliation: Regularly reconcile ATM cash balances to detect and investigate discrepancies promptly.

24/7 Monitoring: Implement round-the-clock monitoring of ATM networks to respond quickly to any signs of fraud or tampering.

Incident Response Plan: Develop and regularly update an incident response plan to address and mitigate any security breaches' impact quickly.

Empowering Your FI Customers, Employees and Institution:

Educational Programs: Develop educational programs or literature to raise customer awareness about ATM security best practices. This includes recognizing skimming devices, using ATMs in well-lit and secure locations, monitoring accounts regularly for suspicious activity, and identifying and avoiding phishing scams. Teach account holders to enable SMS or email alerts for transactions, empowering customers to stay informed and quickly identify unauthorized activity on their accounts. This allows for faster reporting to your institution and minimizes potential financial losses.

Industry Collaboration: Collaborate with other financial institutions, law enforcement agencies, and industry groups to share information and best practices for preventing fraud and theft.

Regulatory Compliance: Maintain high-security levels and ensure compliance with relevant regulations and standards, such as PCI DSS (Payment Card Industry Data Security Standard).

Beyond the Solutions:

Security is not a one-time event; it's an ongoing process. A proactive approach is crucial for comprehensive protection and maintaining your customer's trust. Bolster your overall security position with NuSource and prevent your FI from becoming the latest crime statistic.

For more information or to obtain a comprehensive review of your FIs security posture, contact NuSource today.

Call for more info **952-942-9191**

9749 Hamilton Road
Eden Prairie, MN 55344

nusource.com

sales@nusource.com