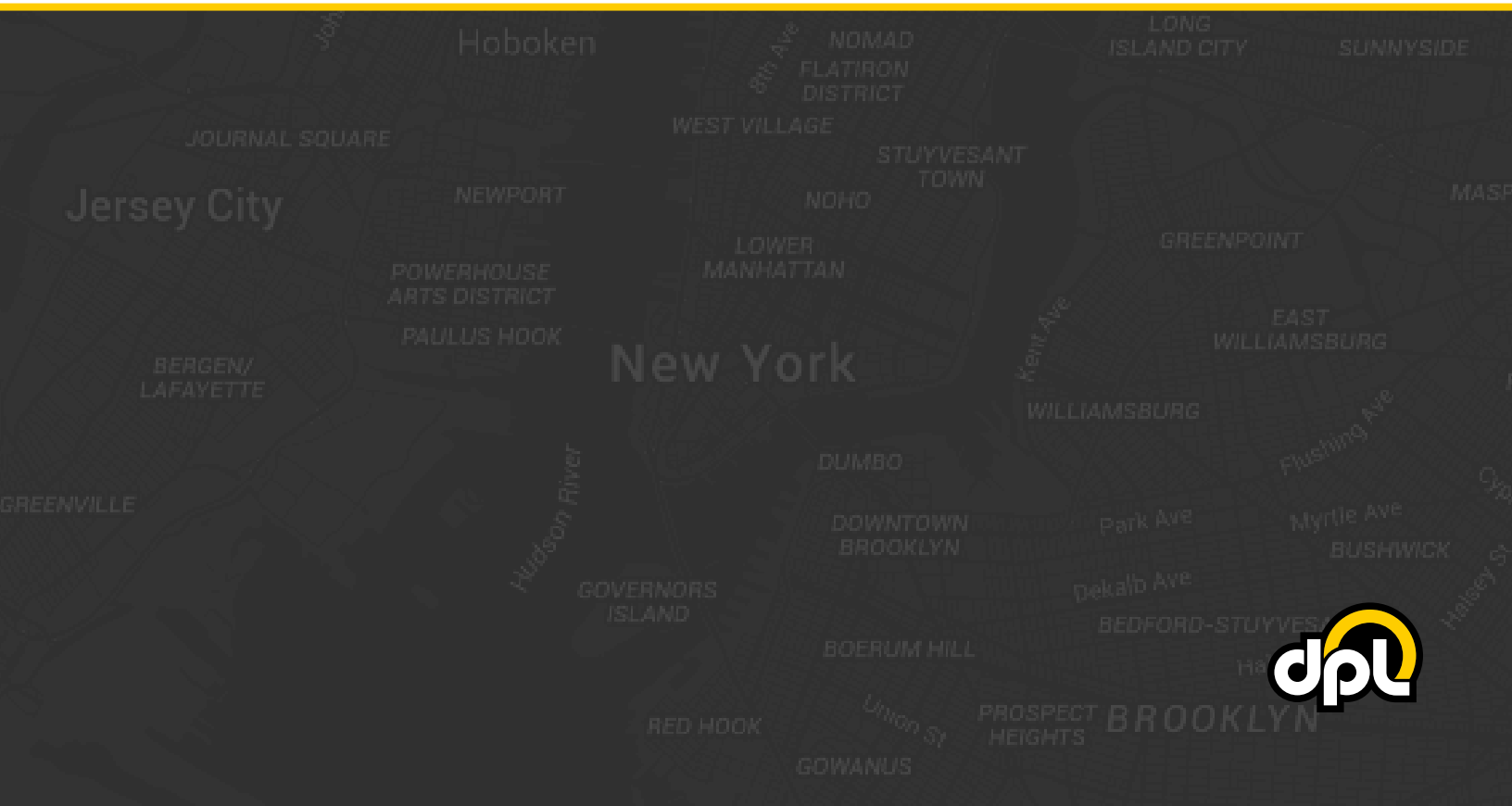
DPL's Comprehensive Guide to ATM Security



Credit: Guelph Mercury Tribune

DPL's Comprehensive Guide to ATM Security

Each year there is an increase not only in the number of ATM attacks but also in the type and extreme nature of attacks.

There are several ATM attack types, usually classified as either a physical or logical attack. Later in this guide we'll expand upon the various types of physical and logical ATM attacks and the steps you can take to avoid them but for now we'll focus on general best practices.

When it comes to protecting ATMs from either physical or logical attacks it's best to deploy a layered approach to security - which means adding several deterrents to protect against multiple types of physical and logical attacks.

Before selecting and deploying security solutions across your entire fleet, first evaluate the types of attacks occurring on a region by region basis. This will allow you to tailor the security solutions you choose to deploy in each region, while controlling the amount of resources dedicated to mitigating risk.

When trying to anticipate what new attack types might make their way to North America, an effective strategy is to follow what's happening in other countries. Many ATM attacks originate from parts of Eastern Europe and South America.

Physical ATM Attacks

Physical ATM attacks are focused on extracting cash from ATMs. These types of attacks happen quickly and often cause a lot of damage to ATMs and locations in the process. Some of the most common physical attacks are:

Ram-raids, Pull Outs, Smash and Grabs - each of these attack types are similar in nature and typically involve using a truck or vehicle as a ramming device to gain entry to a location, physically removing the ATM, then later breaking into the safe and emptying the cash cartridges.

Credit: ATMIA, Best Practices Physical Security V.3

Cutting, Drilling, Wedges, Crowbars and Hydraulic Tools - these types of attacks typically occur at soft targets, where the ATM can be accessed quickly and the cash cartridges are not protected by high grade safes. These attacks involve quickly gaining access to the cash without removing the ATM from its location.

Explosive Attacks - Less common in North America, these extremely dangerous attacks involve using gas or solid explosives to blow up the ATM in order to access the cash.

Physical ATM Security Solutions

Site Assessments - While there are several types of physical ATM attack types, there are just as many security products available on the market to try and protect against them. The first defenses against physical ATM attacks however costs only your time.

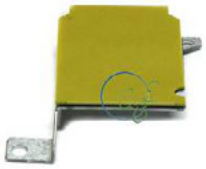
Completing a thorough site assessment of prospective ATM locations can be one of the most effective ways to avoid falling victim to physical ATM attacks. Consider contacting local law enforcement agencies to inquire about crime rates in the area. Interview surrounding business owners and employees to determine whether or not theft and vandalism is a common occurrence in the area.

In addition to assessing the area, give consideration to the physicality of the location itself. If the answers to the following questions cannot be answered favorably you may want to reconsider placing an ATM at the site:

- Can the ATM be positioned in a high visibility area and within the line of site of employees?
- Does the site maintain a functioning security camera system?
- Is the site equipped with its own alarm system and alarm monitoring service?
- Can the ATM be positioned away from easy access points such as doors, windows and exterior walls?
- Is the building constructed from solid materials? (metal, concrete)
- Can the ATM be bolted to the floor or frame of the building?

Once an ATM is installed at a location, perform regular site visits and train location staff on how to perform inspections to ensure it hasn't been tampered with.

Sensors - Installing physical sensors on an ATM that can alert you and others of door open events, tilting and vibration, power cuts and other signs of physical intrusion or tampering can allow you to take immediate action and to notify local law enforcement in the event of an attack. Some providers enable the ability to arm and disarm sensors to avoid being alerted during scheduled maintenance or cash loading.



Credit: American Bank Equipment

Penetration Mats - similar to sensors, penetration mats installed on the fascia of an ATM can alert you if someone is attempting to cut or drill into it.

Credit: PLINTHPAK™

Anchoring devices - Attackers often case locations prior to attacks. One of the things they look for is how easily the ATM can be taken from the location. Bolting an ATM to the floor or securing it to the frame of the building using an anchoring device is an effective way to deter thieves from attempting to steal an ATM.

Security Collars and Anti-lasso Devices - Sometimes bolting an ATM to the floor isn't enough to stop determined thieves from attempting to steal it. In these instances attackers will wrap a chain or rope around the base of the ATM and attach the other end to a vehicle in an attempt to rip the ATM from its foundation. Security collars and anti-lasso devices are designed to stop thieves from being able to place a rope or chain around the ATM.

Tracking Systems - Tracking systems are not designed to stop ATM thefts from occurring. Instead, they're used to try and catch thieves after the crime has been committed. In the event of an ATM theft, tracking devices are used to track the ATMs location. This information can be shared with local law enforcement so they can apprehend those responsible. In many instances it is one person or group of people committing ATM attacks in a particular region and once they are caught thefts stop.

Credit: Lancaster Online

Intelligent Banknote Neutralization Systems (IBNS) A.K.A. Dye or Ink Packs - Designed to render banknotes unusable by thieves, intelligent banknote neutralization systems or dye packs can be built-in to ATM cash cartridges. The ink or dye can be triggered multiple ways; automatically when a cartridge is forcibly opened; when it travels beyond a defined distance from the ATM; within a defined time frame of being in an unsecured state; or upon receiving a remote, user controlled command. If recovered, dyed notes can be exchanged for new ones at the Federal reserve for a small fee.

Audible Alarms and Sirens - similar to dye packs, alarms and sirens can be triggered automatically when a predefined criteria is met or upon receiving a remote, user controlled command. Designed to attract unwanted attention, alarms and sirens can be an effective way to stop thieves mid attack.

Logical ATM Attacks

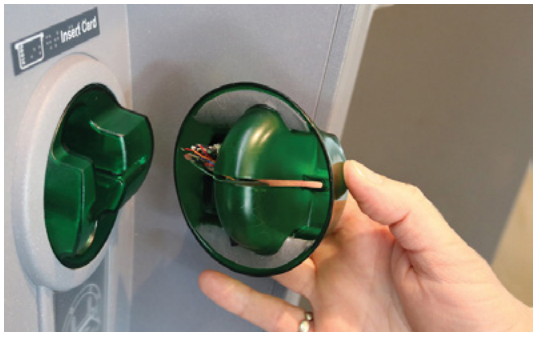
Logical ATM attacks typically have two objectives: 1. Collect card holder information; 2. Manipulate data to fraudulently withdraw money from the ATM. Criminals are always looking for new ways to access cardholder data and to steal money from vulnerable ATMs. Below are some of the logical attacks being used by criminals.

Jackpotting - This refers to emptying all of the money from an ATM. Jackpotting can occur two ways: 1. By gaining control of the bill dispenser and sending it a command to dispense cash. 2. By using a device to intercept and manipulate data being exchanged between the ATM and the payment processor to commit fraudulent transactions.

Black Box, or Man-in-the-Middle - As described above under "Jackpotting", these attacks involve using a third-party device to intercept and manipulate data being sent between the ATM and payment processors to empty some or all of the cash from the ATM. These devices can also be used to read and log cardholder information.

Network Packet Sniffing, and Eavesdropping - These types of attacks use a computer program or computer hardware to intercept and log data being communicated over the ATM network. The data collected can then be used to coordinate and plan other types of attacks on the ATM or to defraud those who have used the ATM to withdraw cash.

Malware - Once installed on an ATMs hard drive, malware can intercept and manipulate data to commit man-in-the-middle or jackpotting attacks and can also log sensitive cardholder information. To install malware, criminals typically need to physically gain access to the ATMs computer hard drive.



Credit: Northwest Community Credit Union

Skimming, Deep Insertion Skimming and Shimming - Designed to read and store card holder information and personal identification numbers (PINs), these types of attacks involve attaching or inserting physical devices to or inside ATMs to read and store information from the cards magnetic strip or EMV chip. This information is then used to clone and create fake debit cards. False PIN pads and cameras are often used to record the users PIN.

Logical ATM Security Solutions

Once again, taking a layered approach to securing ATMs against various types of logical attacks is the best defense. Below are steps you can take to protect your ATMs from logical attacks.

Enable Transport Layer Security (TLS) - TLS is an encryption protocol designed to secure the privacy and integrity of data being transmitted between ATMs and payment processors. When configured correctly, TLS prevents anyone from reading and storing the data or intercepting and manipulating it in any way. IMPORTANT: Simply enabling TLS at the ATM is not enough. Once enabled be sure to also enable TLS certificate validation and confirm that the correct TLS certificates are configured on ATMs.

Changing Locks - Out of the box, ATMs from the same manufacturer typically use a universal key to provide access to top hats. This is where the computer, hard drive (if applicable), USB ports, and connections to items such as bill dispensers are housed. While changing the locks across your entire ATM fleet may seem daunting, securing the top hats is your first line of defense against criminals trying to compromise the cyber security of your ATMs. Once locks are changed, make duplicate keys, label and distribute them to any third party vendors requiring access to your ATMs and request vendors notify you if a key is lost so you can change the lock and issue them a new key.

Secure Communications Sockets and Access Ports™ - Unsecured entry points like communication sockets and access ports for running power to ATM toppers provide easy access to USB ports, Ethernet connections and bill dispenser jacks. Criminals have been known to fish confined space tools (snakes, forceps etc,) into ATMs to install malware, packet sniffing devices and launch other types of logical attacks. Use the communication socket plugs provided by manufacturers to protect ATMs from being easily compromised.

Encrypt Hard Drives (if applicable) - ATMs with support for hard drive encryption should be encrypted to prevent criminals from being able to modify the drive while it is offline or removed, and to prevent the installation of malware or network sniffing software.

Keep Firmware and Software Up-to-Date - Periodically ATM manufacturers release firmware updates to address security issues. Similarly operating system software companies release security patches. It's important to keep ATMs up-to-date with the latest firmware and your systems updated with software updates to protect them from attacks.

Enable Message Authentication Codes (MAC) - In some countries, like Canada, payment processors issue MAC keys to IADs to configure in each ATM. A MAC key is a secret key used to confirm that the message came from the stated ATM and has not been manipulated. The MAC value ensures a message's data integrity as well as its authenticity by allowing payment processors and ATM (who both possess the secret key) to detect any changes to the message. Bottom line is that if MAC keys are used, host authorization manipulation jackpotting attempts will be unsuccessful.

Upgrade ATMs to be EMV Compliant - Most modern ATMs purchased today are EMV compliant, meaning they seek to validate users' PINs as well as authentication data encrypted on EMV chip enabled cards. Older, non EMV compliant ATMs make it possible for criminals to use cloned cards, as they do not validate EMV authentication data. IADs are considered to be liable for fraud committed at non EMV compliant ATMs. Most ATMs can be upgraded to be EMV compliant by replacing the card reader and updating the ATMs firmware or software.

Sensors - Similarly to protecting against physical attacks, sensors placed on ATMs can detect and alert for early physical signs of tampering related to logical attacks. Early tampering detection allows you to take immediate action to stop attacks in their tracks and increase your chances of catching those responsible.

Position ATMs in Highly Visible Areas - Placing ATMs in highly visible areas, within the sight-line of location employees and security cameras, can significantly decrease the likelihood of both physical and logical attacks from occurring. If criminals think there is a chance someone might see them in the act, they're less likely to attempt it in the first place.

Conduct Regular ATM Inspections - Train service technicians and location employees on how to identify signs of tampering and have them perform regular inspections of the exterior and interior of ATMs. Have them check for fake keypads, cameras and devices placed over the mouth of card readers or in-line with communication cables. Early detection of tampering can disrupt fraudulent activity before it's too late.

DPL's Custom Security Solutions

We hope you've found the information contained within this guide useful. To help our customers protect their businesses against attacks, we've designed and manufactured security solutions specifically for ATMs.

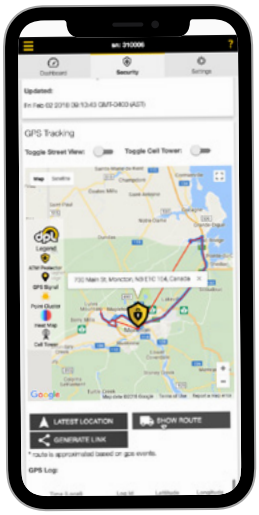
Protector GPS

Know What's Happening at Your ATMs

PROTECTOR GPS

Receive multi-recipient alerts via text, email, telephone and in the Hercules Portal for:

- Power Cuts
- Tilting & Vibration
- GPS Movement
- Door Open Events



Once alerted, log in to the mobile friendly Hercules Portal to view alarm details and track your ATM's GPS position. Share a secure link with local law enforcement so they too can track your ATMs GPS position in real time.

The Protector GPS's internal battery can last up to 8 days when fully charged.

For more information visit:

dplwireless.com/atm-protector

Comming Soon!

ATM Cash Guard

The ATM Cash Guard works in conjunction with all of our Hercules wireless ATM modems and gives IADs the ability to cut power to ATM bill dispensers and the entire ATM in the event of physical or logical attack.

Hercules Shield - Coming Soon!
Wireless Connectivity and Security In One

The Hercules Shield will offer the same reliable wireless connectivity our customers have come to trust from our Hercules modems, plus built-in GPS, intrusion detection and physical security capabilities. Additionally it will feature our proprietary NTrap™ Ethernet ports, uniquely designed to be able to detect physical tampering at the lowest level.

Able to support dual carrier and dual SIM, the Hercules Shield will be able to send multi-recipient alerts via text, phone and email for early signs of physical, logical or black box attacks such as:

- GPS Movement
- Tilting and Vibration
- Door Open Events
- Ethernet Tampering
- IP Address Change
- MAC Address Change
- ATM Connection Lost
- Power Interruptions

All of this packed into the same rugged, metal, space-efficient Hercules case!

If you have questions related to ATM security or want more info about our products and services, please call us at 1-800-561-8880 or email sales@dplwireless.com

CALL NOW
1-800-561-8880