Best Practices for Customer Security Education

International Minimum Security Guidelines and Best Practices for Protecting ATM Systems

Produced by the ATM Industry Association

Contributors:

e-mail Mike Lee, ATMIA's CEO, at mike@atmia.com

Disclaimer

The ATM Industry Association (ATMIA) publishes *Best Practices for Customer Security Education* in furtherance of its non-profit and tax-exempt purposes to promote increased protection for ATMs through research-based education. ATMIA has taken reasonable measures to provide objective information and recommendations to the industry but cannot guarantee the accuracy, completeness, efficacy, timeliness or other aspects of this publication. ATMIA cannot ensure compliance with the laws or regulations of any country and does not represent that the information in this publication is consistent with any particular principles, standards, or guidance of any country or entity. There is no effort or intention to create standards for any business activities. These best practices are intended to be read as recommendations only and the responsibility rests with those wishing to implement them to ensure they do so after their own independent relevant risk assessments and in accordance with their own regulatory frameworks. Further, neither ATMIA nor its officers, directors, members, employees or agents shall be liable for any loss, damage or claim with respect to any activity or practice arising from any reading of this discussion paper; all such liabilities, including direct, special, indirect or inconsequential damages, are expressly disclaimed. Information provided in this publication is "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or freedom from infringement. The name and marks ATM Industry Association, ATMIA and related trademarks are the property of ATMIA.

Please note this discussion paper contains confidential information and should not be left lying around or freely copied without due care for its distribution and safekeeping.

Table of Contents

Foreword

In a major future-proofing exercise undertaken by the ATM industry, the Consortium for Next Gen ATMs, represented by just under 150 companies worldwide across all sectors of the ATM value chain, has agreed that the main way of transacting at ATMs in the future will be through the customer's mobile device/smartphone. We expect an API APP model for ATMs to become the norm whereby customers will use bank apps to pre-stage ATM transactions so that the actual transaction at the terminal will be faster and more personalized than ever before. The idea is to enhance the customer experience.

This means, however, that the industry will need to educate customers on how to protect their own Customer Owned Devices (CODs) as the means of transacting with ATMs rather than using a plastic card. Customers have always been an important part of fraud prevention in financial services, but in the future their role will be central, necessitating a new paradigm with greatly increased education on security tips conveyed to bank customers.

This manual takes best practice from financial institutions around the world and distills the essence of security education for today's and tomorrow's ATM customers. It explores typical methods of attack, current protection measures in place, customer security tips as well as best-to-communicate core security messages to customers.

This manual is the first step ATMIA has taken to ensure security best practices are built into the next gen ATM project from its inception. As the actual ATM architecture is signed off by the Consortium, our security subcommittee will identify additional best practices required for the whole new ATM ecosystem.

Mike Lee, CEO ATMIA

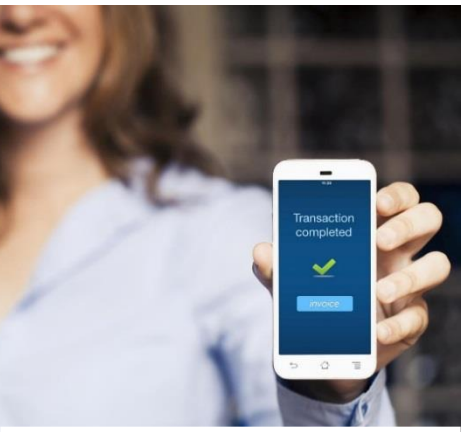
April 2018

Executive Summary

Please note that this "Executive Summary" cannot replace reading the entire manual. The summary is merely a guide to the content and main principles of these best practices.

The aim of this guide is to help ATMIA members identify and communicate key security messages that enhance customer confidence and empower customers to transact safely and securely.

- The way customers interact with ATMs is rapidly changing. The integration with other financial services channels, such as mobile and internet banking, continues to strengthen. Customer Owned Devices (CODs) will increasingly be used as customers interface with ATMs.
- Defending against criminal attacks cannot be truly effective unless customers transact in a secure way.
- Customer education is absolutely key in ensuring customers have the knowledge and skills to achieve the highest level of security possible while enjoying the convenience of ATMs and other integrated financial services channels.
- Global research has identified some of the most effective customer education strategies and methods that can enhance knowledge and encourage behavior that protects customers.
- For each channel there are four key factors that are considered:
  - Common Scams
  - Protection Measures
  - Message Placement
  - Key Security Education Messages
- Advising customers about the type of real-life scams that occur can decrease their chances of becoming victims.
- Communicating the range of protection measures deployed can significantly raise customer confidence.
- Considering the placement of messages identifies opportunities to deliver key messages most effectively.
- Delivering simple and clear education messages can make it more likely customers will remember to transact securely.



Defending against criminal attacks cannot be truly effective without customers playing their role.

Acknowledgements

ATMIA is indebted to Douglas Russell, DFR Risk Management, for the creation of this *Best Practices*, which highlights the latest globally-effective customer security education advice reflecting the convergence of the ATM channel with Customer Owned Devices (CODs).

Additionally, we would like to thank the ATMIA Consortium for Next Generation ATMs Subcommittee on Security for reviewing the *Best Practices* document and, in particular, Liza Horowitz, SPL Group, and Leland Englebardt, Upshot Advisors, for their contributions.

Chapter 1. Introduction

The ATM industry and card issuers are constantly investing and enhancing their systems to defend against an ever-expanding range of criminal attacks. The sophistication of attacks against ATMs range from the relatively simple, non-tech methods to highly advanced types of cyberattack.

The way customers interact with ATMs is rapidly changing. While traditional methods of interacting with ATMs, such as card and PIN, will continue to be a primary method for obtaining cash and other services at ATMs, the integration of other financial services channels, such as mobile and internet banking, continues to strengthen. In particular, CODs will increasingly be used as customers interface with ATMs.

Customer education is absolutely key in ensuring customers have the knowledge and skills to achieve the highest level of security possible while enjoying the convenience of ATMs and the other integrated financial services channels.

Defending against criminal attacks cannot be truly effective unless customers transact in a secure way. Customer education is absolutely key in ensuring they have the knowledge and skills to achieve the highest level of security possible while enjoying the convenience of ATMs and the other integrated financial services channels.

This Best Practices guide is the result of global research, which identified some of the most effective customer education strategies and methods that can enhance knowledge and encourage behavior that protects customers.

The key channels of ATM and CODs are looked at individually before being consolidated into a channel-agnostic collection of key best practice behaviors.

For each channel there are four key factors that are considered:

- Common Scams
- Protection Measures
- Message Placement
- Key Security Education Messages

Educating customers about real-life examples of the types of scams they might be exposed to can immediately raise awareness, which can lead to victim avoidance.

Communicating the range of protection measures deployed can significantly raise customer confidence that the channel owners are committed to protecting customers.

Considering the placement of messages identifies opportunities to deliver key messages at the most effective time and place when a transaction is being prepared or performed.

Simple and clear education messages can make it more likely that customers will remember to transact securely.

Chapter 2. ATM Specific

2.1. Common ATM Scams Targeting Customers

Advising customers about the types of real-life ATM scams that occur can help them to recognize when something is suspicious and decrease their chances of becoming victims. It is important to choose the types of scams that are likely to be recognized as such, rather than simply listing every conceivable method, many of which the average customer would be unlikely to recognize as a scam.

Broadly speaking, ATM scams can be classified under fraud, physical attacks and logical attacks. Skimming falls under ATM fraud and is the most popular method to steal card information, clone cards and empty a person's bank account. Physical attacks include ATM sabotage. Logical attacks occur when perpetrators gain access to the inside of the ATM.

Image Courtesy of SPL Group

2.1.1. Skimming

Skimming involves a device that can make a copy of the information on the card's magnetic stripe. Skimming devices can be attached over the card entry slot at an ATM or can be a device held manually by the perpetrator. Customers should be suspicious of unusual additions or changes to the ATM card entry slot, particularly if the slot seems loose or damaged. Customers should also be suspicious of anyone attempting to gain access to their card when transacting at ATMs. If customers' cards are not already EMV chip cards, they should request one from the issuer.

2.1.2. Card Swapping

Perpetrators are known to offer assistance to customers who have difficulty using the ATM. Customers should be suspicious of helpful strangers and not allow anyone to touch their card. Helpful strangers are known to exchange or swap the customer's card with another of similar appearance.

2.1.3. Card Trapping

Card trapping involves a device fitted to or inside the card slot that prevents the card from being ejected and returned to the customer. Customers should be suspicious if the ATM appears to have swallowed their card and avoid accepting any help or advice from strangers, especially if the stranger suggests the card will be returned if the card owner enters their PIN again. Customers should immediately contact their issuer to report the card as missing.

2.1.4. Shoulder Surfing

Perpetrators can try to watch customers entering their PIN. Customers should be suspicious of strangers standing too close to them at an ATM.

2.1.5. Spy Cameras

Miniature spy cameras can be attached to the ATM to make a video recording of customers entering their PIN. Customers should be suspicious of any additional devices attached to the ATM, particularly if they seem to be loose or damaged.

2.1.6. Fake PIN Pad Overlays

Perpetrators can attach fake PIN pad overlays and fake keyboards over the genuine ATM PIN pad or keyboard to record PINs. Customers should be suspicious if the PIN pad or keyboard seems loose or damaged, or the keys feel very stiff when entering their PIN.

Image Courtesy of SPL Group

2.1.7. Distraction

Distraction techniques are used to divert a customer's attention while performing a transaction. The purpose is usually to steal cash or the ATM card. A common method includes dropping some cash and asking if it belongs to the customer. An accomplice steals the cash or card while the customer is distracted.

2.1.8. Cash Trapping

Cash trapping devices are designed to hold back dispensed cash, leaving the customer to believe the ATM made an error. Perpetrators either insert a trapping device over the cash shutter or within the cash dispenser. After not receiving the dispensed cash, the customer leaves, and the perpetrator returns to collect the cash. Internal trapping devices can be designed to collect money dispensed from several customers. Customers should check their balance and immediately notify their issuer if it has been debited for cash not received.

2.2. Protection Measures Deployed

While recognizing that individual ATM deployers and card issuers have different levels of security, highlighting some of the primary defenses they deploy can help increase customer confidence. Examples might include:

- EMV chip card support
- Geo-blocking of foreign ATM transactions
- Monitoring for unusual transactions
- Anti-skimming technology

- Mirrors to view persons behind the customer
- Regular inspection of ATMs
- Remote monitoring of ATM devices
- Transaction cameras and area CCTV
- 24-hour emergency telephone number
- SMS transaction alerts

2.3. Message Placement Opportunities

In addition to providing regular customer education messages along with correspondence from card issuers, such as statements, graphical messages can be displayed on the ATM screen and printed on ATM paper receipts.

2.4. Key ATM Security Education Messages

The following are examples of key educational messages relevant to the security of ATM transactions:

- Never give anyone your PIN.
- Cover the keyboard when entering the PIN.
- Never write your PIN on the card or keep it with your card.
- Choose a PIN difficult to guess; avoid personally-identifiable information, such as birthday, ID number and telephone numbers.
- Don't allow someone to help you with a transaction.
- Check that no one is very close to you when performing a transaction.
- Choose an ATM in a well-lit location, and have your card or device ready for use.
- Do not use an ATM if you are suspicious or it looks damaged.
- Cancel the transaction, take your card and leave the ATM if you feel uncomfortable for any reason.
- Add your card issuer's emergency number to your cell phone contacts list.
- If you observe anything unusual or suspicious about an ATM transaction you have done or attempted to do, immediately report it to your card issuer using your own contact information (not a telephone number attached to the ATM). Examples of unusual ATM behavior include:
  - Your card is not returned,
  - Your cash is not delivered, or
  - You do not receive a receipt when you request one.

Customers should be suspicious of unusual changes to the ATM.

Photo Courtesy of NewMoney

- Check transaction records frequently, and report suspicious transactions immediately.
- Subscribe to SMS transaction alerts.
- After completing a transaction, make sure you have your own card.
- Pay attention. Do not allow yourself to be distracted while performing a transaction.
- Never give card, device or PIN details to anyone, even if they claim to be an official. Your genuine card issuer will never ask you for these details in person or by phone, SMS, email or website.

Chapter 3. Customer Owned Devices

3.1. Common Scams Targeting CODs

Advising customers about the types of real-life scams involving CODs, including smart phones, tablets and PCs, can help them to recognize when something is suspicious and decrease their chances of becoming victims. It is important to choose the types of scams that are likely to be recognized as such, rather than simply listing every conceivable method, many of which the average customer would be unlikely to recognize.

3.1.1. Rogue Banking Apps

Rogue banking apps are designed to look like the genuine app but contain malicious software that can intercept and steal a customer's private information. Perpetrators often promote the rogue banking apps through email and fake websites.

3.1.2. Rogue General Apps

Apps not specifically designed to look like a banking app have been known to contain malicious software that can intercept and steal a customer's private information. Perpetrators often promote the rogue apps as freeware.

3.1.3. Malicious Software

Malicious software (malware) is often specifically designed to steal secret information when customers are transacting with services, such as on-line banking. "Keyloggers" can copy customers' keystrokes and redirect them to fraudulent websites. Malware is commonly hidden in free-to-download (freeware) software.

3.1.4. Free WiFi

Perpetrators can monitor unsecured WiFi hot spots and intercept private data when a COD connects to it. Most public spots are unsecured, including coffee shops and malls. Even apparently-secured public WiFi services can be compromised.

3.1.5. Theft of CODs

CODs are frequently stolen from public areas, including by teams of pickpockets. Perpetrators have used stolen CODs that are not sufficiently secured to perform financial transactions and steal private data.

3.1.6. SIM Porting and Swapping

Perpetrators use social engineering and trickery to obtain enough personal information to enable them to port the customer's COD telephone number onto a device the perpetrators control. Once the telephone number is ported, customers will no longer receive SMS transaction alerts and One Time Passwords (OTPs).

3.1.7. Phishing

Perpetrators are known to trick customers into divulging secret information or transferring money to persons emailing them and claiming to be from their card issuer or bank. Techniques include claiming that the customers' account has been compromised and advising that they should transfer their balance into a "safe account." A common characteristic is that the message is urgent and needs immediate action. Links within the phishing email often take customers to fraudulent websites.

3.1.8. SMiShing

SMiShing is similar to phishing. Perpetrators send rogue SMS text messages to customers' CODs to trick them into divulging secret information or transferring money. A common characteristic is that the message is urgent and needs immediate action.

3.1.9. Vishing

Vishing is similar to phishing, but the perpetrator calls the customer by telephone to obtain secret information or to trick the customer into performing a transaction or to take a specific course of action.

3.1.10. Text Bomb

A text bomb is a malicious text message which can cause CODs to crash. Perpetrators can use text bombs to prevent customers from receiving genuine SMS transaction alerts.

3.1.11. Fraudulent QR Codes

Perpetrators use fraudulent Quick Response (QR) codes to trick customers into visiting certain websites or transferring money into a criminal's account. Fraudulent QR codes can be physically overlaid onto genuine QR codes, and they can be sent by email.

3.2. Protection Measures Deployed

While recognizing that individual service providers and card issuers have different levels of security, highlighting some of the primary defenses they deploy can help increase customer confidence. Examples might include:

- Strong end-to-end encryption
- Independently-assessed secure app
- Provision for free security software
- Monitoring for unusual transactions
- Prevention of loading onto “jailbroken” or “rooted” devices
- Regular updates to the app to enhance security
- App support for long security codes
- App support for biometric authentication methods
- Customer-defined limits to transaction values
- OTPs for particular transactions
- Multifactor authentication methods
- SMS transaction alerts

3.3. Message Placement Opportunities

In addition to providing regular customer security education messages, along with correspondence from card issuers, such as statements, graphical messages can be displayed on the device’s screen. Animation can be used to demonstrate safe transacting when the app or on-line banking software is first installed and updated.

3.4. Key COD Security Education Messages

Following are key customer security education messages relevant to CODs:

- Set a strong password or code to unlock the device.
- Set a code to unlock your SIM.
- Ensure passwords or codes are unique for your device and not used for ATM PIN or other services and devices.
- Use biometric unlock if supported by the device.
- Set auto-lock and time-outs to a minimum time.
- Only download apps from an official app store, and use caution when downloading apps. Take certain precautions, especially when you need to enter financial information. Here are a few tips to determine if the banking app you are downloading is the verified version:
    - Check app reviews.

  - Check the number of downloads.
  - Look at the app publisher.
  - Look at the publish date – be wary of new apps.
  - Look for spelling mistakes; banks have rigorous communication checks.
  - When in doubt, go to bank's website and go to "get our app."
- Only download PC software from the official bank website.
- Use the official mobile app rather than mobile browsers.
- Do not "jailbreak" or "root" your device.
- Do not let others use your device.
- Use only your own device to transact.
- Do not use public shared computers.
- After using the app or on-line service, log out and close.
- Clear browser cache and disable auto-fill.
- Do not store a record of passwords, codes or account details on the device.
- Protect your device and any OTP generators provided.
- Use 3G/4G rather than free WiFi connections.
- Consider using a trusted Virtual Private Network (VPN).
- Disable WiFi, Bluetooth and NFC when not required.
- Secure your own WiFi to the highest level permitted.
- Do not allow others to observe your unlock details and codes; be vigilant to possible observation by CCTV in public places.
- Keep your device up-to-date with operating system and application patches.
- Install and keep up-to-date anti-malware defenses.
- Configure a personal firewall.
- Report lost or stolen devices and have them blocked, if applicable.
- If an unexpected loss of the cell phone network occurs, consider the possibility your number has been illegally ported/swapped to a criminal's device.
- Be suspicious of sudden poor performance or poor battery life after installing new apps or software; they may contain malware.
- If your device needs to be repaired, remove all financial apps and details, and advise the issuer to block the device, if applicable.
- Enable remote locking and wiping in case your device is lost or stolen.

It is vital that customers secure their mobile devices.

Chapter 4. Integrated Channel

While channel-specific customer education is important and provides an opportunity for a more in-depth focus to enhance the knowledge and skills of those using financial services, it can help to communicate some key points at a higher level. Following are five examples:

1. Your details are private: KEEP THEM SECRET.
    - PINS
    - Passwords
    - OTPs
    - Account details
2. Your access device is valuable: SECURE IT AND PROTECT IT.
    - Cards
    - Mobile
    - Tablet
    - PC
3. It's your money: DON'T LET SOMEONE TRICK YOU.
    - Helpful stranger
    - Phishing
    - SMiShing
    - Vishing
4. Be aware: REPORT SUSPICIONS IMMEDIATELY.
    - Transaction monitoring
    - SMS transaction alerts
    - Lost and stolen reports
5. Stay safe and don't be rushed: TRUST YOUR INSTINCTS.
    - Well-lit area
    - Condition of ATM
    - Private setting

Chapter 5. Further Reading and Links

ATMIA Best Practices:
https://www.atmia.com/best-practices/

ATMIA Alerts:
https://www.atmia.com/education/security/fraud-alerts/