



Evidence Solutions, Inc.
&

Netzel Financial

Present:

ATM Card Skimming and PIN capturing
What to look for and how to avoid being a victim.

October 20, 2011

Presented by:

Scott Greene, SCFE, CEO
Evidence Solutions, Inc

520-512-5001
866-795-7166

Scott@EvidenceSolutions.com

Biography

Scott Greene

For more than 20 years, Scott Greene has been helping CEO's, business owners and managers, and IT departments meet the challenges in the swiftly evolving computer industry. He is the founder of Great Scott Enterprises, Inc., an Arizona based firm, which provides superior full service computer consulting services. The array of services includes custom programming, design optimization and administration of databases, evaluation of existing systems to ensure optimal efficiency and profitability, and designing and implementing knowledge base systems.

This experience is what draws clients to him from all over the United States for consulting in the field of Computer Forensics which has become a rapidly growing field of endeavor. His extensive and diverse experience allow him to be an expert in many facets of computer technology. He is a sought after speaker on the subject and has presented to all of the major Bar associations in Arizona and other legal, accounting and security associations throughout the Southwest.

In 2008 Great Scott Enterprises, Inc. created Evidence Solutions, Inc. as the Technology Forensics division of Great Scott Enterprises, Inc.

ATM Card Skimming and PIN capturing

Faculty:
Scott Greene
of
Evidence Solutions, Inc.

Scott@EvidenceSolutions.com

www.EvidenceSolutions.com

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.

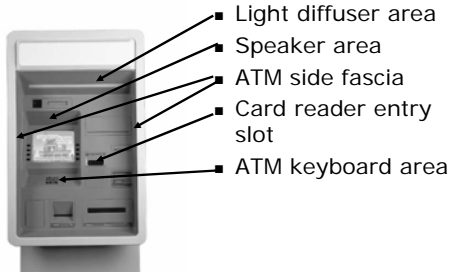


What is Skimming?

- **ATM Card Skimming** is a method used by criminals to capture data from the magnetic stripe on the back of an ATM card.
- The devices used are smaller than a deck of cards and are often fastened in close proximity to or over the top of an ATM's factory-installed card reader.
- **Pin Capturing** refers to a method of strategically attaching cameras and various other imaging devices to ATMs; in order to fraudulently capture the ATM user's PIN.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



- 
- Light diffuser area
 - Speaker area
 - ATM side fascia
 - Card reader entry slot
 - ATM keyboard area


© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.







What do skimming devices look like?



- Normal flashing lead light.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics. esi



© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



What do skimming devices look like?

- A skim device has been installed on the card reader slot. Although it has the appearance of a standard part of the terminal it is not.
- Note: No flashing lead through light can be seen. The shape of the bezel is clearly different.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



What do skimming devices look like?

A photograph showing a close-up of an ATM's card reader area. A hand is visible, pointing towards the card reader slot. A small, rectangular device is installed on the card reader slot, which is a skimming device. The device is integrated into the ATM's interface.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



What do skimming devices look like?



© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.





© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



What about Pin Capturing?



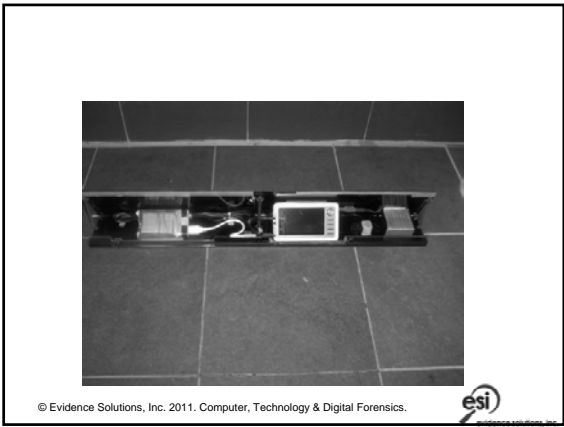
© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.





© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.





© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.





© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



How about now?



© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



A Clever Pin Capture Device



© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



Remove the marketing material...



© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



Skimming Facts

- Criminals tend to attach skimming devices either late at night or early in the morning, and during periods of low traffic.
- Skimming devices are usually attached for a few hours only.
- Criminals install equipment on at least 2 regions of an ATM to steal both the ATM card number and the PIN.
- Criminals then sit nearby receiving the information transmitted wirelessly via the devices (installed on the ATM).

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



Steps you can take

- Get to know the appearance of your Bank's ATM
- Inspect the front of the ATM for unusual or non standard appearance.
- Scratches, marks, adhesive or tape residues could be indicators of tampering
- Flush with the front!

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



Steps you can take.

- Pay attention to all of the touch and action points. (e.g. keypad, customer card entry slot, lighting diffusers)
- Look at card reader entry slot & regions immediately above the consumer display and keyboard area for anything unusual.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



Other Skimming Devices



© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



ATM Cash-point Scams using "Lebanese Loop"

- A scam involving ATM machines in which thieves insert clear plastic sleeves into the machine's card slot.
- How it works:
 - Unsuspecting customer inserts his or her card and enters their PIN
 - Multiple prompts to enter the PIN
 - The system can't read the magnetic strip.
 - After several unsuccessful attempts to reenter the PIN, the user finds that he or she cannot remove their card
 - The customer leaves the machine mistakenly believing that the machine has malfunctioned and retained their card.
 - Usually another customer is present who views the PIN.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.






© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.






If your card doesn't come out:

- Examine the card slot and run your fingers across it to find one or more of the almost imperceptible "prongs" attached to the plastic sleeve that are designed to permit the thief to remove it.
- Do not assume that the machine "ate it". If you have a cell phone, remain at the machine and call the telephone assistance number listed on it.
- If an "ATM repairman" or someone identifying himself as "a police investigator" who retrieves the card from the slot, do not turn that card over to them for any reason, most notably for "evidentiary purposes".
- Con artists often pose as repairmen, police investigators and even FBI agents; legitimate law enforcement officers will never ask you to turn over your ATM card, credit card, or cash.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics. 

Other ATM Scams...

- In one case a bogus female bank employee stood next to an ATM promoting a drawing in which cardholders were entered to win a prize.
- The customer's names were written on the back of transaction receipts which were placed in a box.
- Little did they realize that their PIN codes were being observed and recorded.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics. 

Other things to know:

- Know what your daily limit is
- Review your statements
 - If traveling abroad, have someone review your statements.

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.



Scott Greene, SCFE
Evidence Solutions, Inc.
866-795-7166
Scott@EvidenceSolutions.com

© Evidence Solutions, Inc. 2011. Computer, Technology & Digital Forensics.





Seminar Evaluation Form

Date: _____

	Poor	Ok	Good	Very Good	Excellent
1. Was the material informative?	1	2	3	4	5
2. Was the material easy to understand?	1	2	3	4	5
3. Was the material appropriate?	1	2	3	4	5
4. Was the material interesting?	1	2	3	4	5
5. Was the medium used to present this subject effective?	1	2	3	4	5
6. The material presented in the seminar will be of use to me.	1	2	3	4	5
7. The material presented was properly sequenced.	1	2	3	4	5
8. Was the speaker effective?	1	2	3	4	5
9. The seminar was well worth my time.	1	2	3	4	5
10. Have you relied on computer forensics in your previous experience?				YES _____	NO _____

12. General impression of material presented? _____

13. Why did you attend this seminar today? _____

14. Would you like someone to contact you about computer forensics? YES _____ NO _____

Name: _____

Address: _____

Mailing Address: _____
 (if different)

Email: _____

Phone: () _____ Fax: () _____

Comments may be used on EvidenceSolutions.com. Please let me know if you object.