Cyber Security for Small Businesses

Andy Green, Ph.D. Candidate(ABD),
Operations Manager
Center for Information Security Education

Presentation Overview

- My background
- Introduction
- What to protect
- What threats are out there
- How to lessen vulnerabilities and risk
- How to respond to an incident

My background

- Been doing Information Security (InfoSec) about 15 years or so
- Owned my own InfoSec consulting firm for last 10 years or so, SMB clientele
- Working on my dissertation, so I basically never sleep…

My background

- Volunteer with National Veterans Wheelchair Games since 2007
- Really grateful for the opportunity to talk to you nice people today!
- Roll Tide!

Introduction

- 2012 SBA report on Georgia highlights:
  - Small businesses employed 1.5 million workers in 2010, mostly from firms with 20-499 employees
  - Most businesses are very small – 81.9% have no employees; most employers have fewer than 20 employees
  - Veteran self-employment fared the best
  - 2011 proprietors' income of $27.2B

Introduction

- All these numbers point to what we refer to as a “target rich environment” for attackers of various types
- Target has shifted from large-scale enterprises to local “mom and pop” shops
- Easier to compromise, but have to hit more of them

Introduction

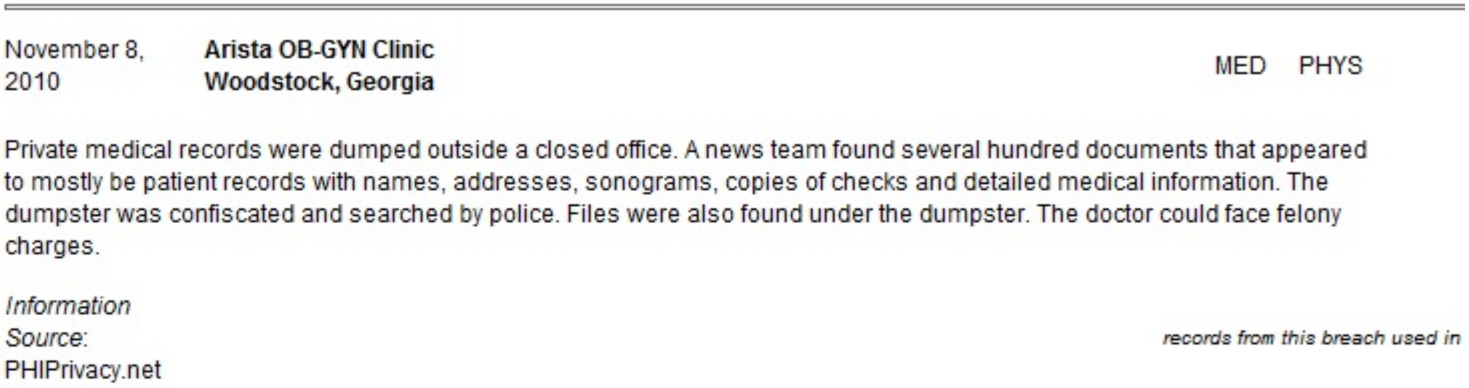
- We read about Target, Neiman Marcus, etc…
- Who covers the theft from “Joe’s Hammer Emporium” located on Main Street?

NOBODY!

What to protect

- Banking accounts
- Credit cards
  - Yours
  - Customers
- Employee records
- Customer data
- Intellectual property (IP)
- Sensitive company data

What to protect



November 8, 2010

Arista OB-GYN Clinic
Woodstock, Georgia

MED PHYS

Private medical records were dumped outside a closed office. A news team found several hundred documents that appeared to mostly be patient records with names, addresses, sonograms, copies of checks and detailed medical information. The dumpster was confiscated and searched by police. Files were also found under the dumpster. The doctor could face felony charges.

Information Source: PHIPrivacy.net

records from this breach used in

What threats are out there

- Social engineering (SE) scams
- Network breaches
- Physical breaches
- Mobile breaches

What threats are out there

- Social engineering (SE) scams
  - “Hacking the human”
  - Phishing and spear phishing attacks
  - “Watering hole” attacks
  - Telephone calls as setup for other attacks

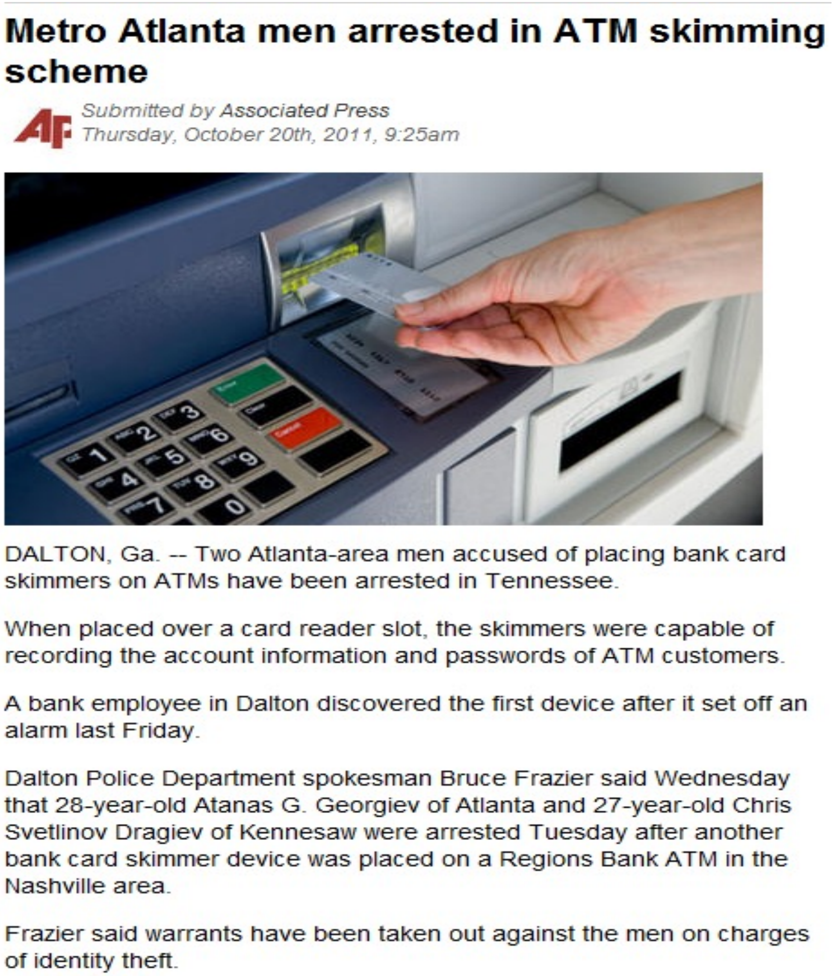
What threats are out there

- Network breaches
  - Malware
  - Unsecured Internet connections
  - Weak (or no), reused passwords
  - Bad (or no) encryption

What threats are out there

- Physical breaches
  - Device theft and/or loss
    - Laptops, mobile devices, tablets
    - Business office breaking and entering
  - Foreign contact
    - Devices confiscated at border, or being forced to display encrypted content

What threats are out there



Metro Atlanta men arrested in ATM skimming scheme

Submitted by Associated Press
Thursday, October 20th, 2011, 9:25am

DALTON, Ga. -- Two Atlanta-area men accused of placing bank card skimmers on ATMs have been arrested in Tennessee.

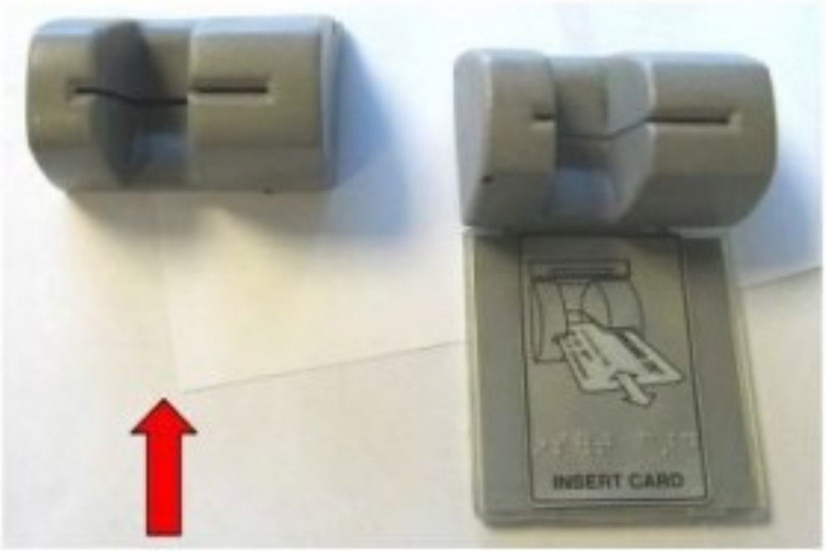
When placed over a card reader slot, the skimmers were capable of recording the account information and passwords of ATM customers.

A bank employee in Dalton discovered the first device after it set off an alarm last Friday.

Dalton Police Department spokesman Bruce Frazier said Wednesday that 28-year-old Atanas G. Georgiev of Atlanta and 27-year-old Chris Svetlinov Dragiev of Kennesaw were arrested Tuesday after another bank card skimmer device was placed on a Regions Bank ATM in the Nashville area.

Frazier said warrants have been taken out against the men on charges of identity theft.

What threats are out there

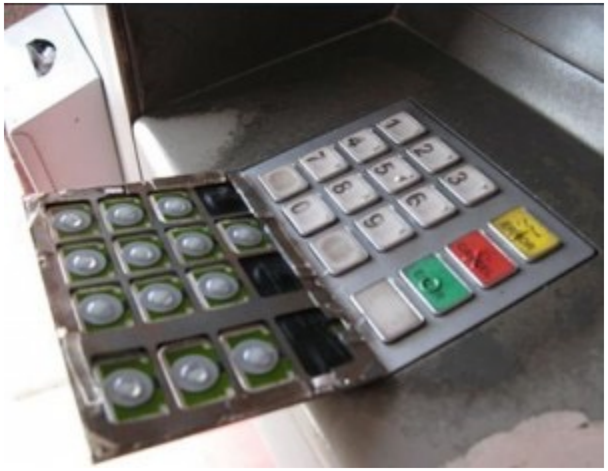


The real card reader slot.

The capture device

Source: http://krebsonsecurity.com/all-about-skimmers

What threats are out there



ATM PIN capture overlay device pulled back to reveal legitimate PIN entry pad

Source: http://krebsonsecurity.com/all-about-skimmers

What threats are out there

A bogus PIN pad overlay

Bluetooth-enabled gas pump skimmer

Source: http://krebsonsecurity.com/all-about-skimmers

What threats are out there

- Mobile breaches
  - “Got an app for that”?
    - Data leakage
    - Malicious code
  - Web-based threats
  - Network threats
    - Is “starbucks” really “starbucks”
    - Man-in-the-middle (MiTM) attack or packet sniffing

How to lessen vulnerabilities and risk

- Assume you are a target
- Secure your banking processes
  - In-person is best
  - Set up automated notifications via email or SMS
  - Segregate duties
  - Multi-factor authentication if online banking

How to lessen vulnerabilities and risk

- Defend yourself!
  - Firewalls
  - AV software
  - Securely connect to the Internet
- Educate yourself and your employees

How to lessen vulnerabilities and risk

- Locate and protect your data
    - Encrypt
    - Limit access
    - Back up offsite
- Account credentials
    - Strong passwords
    - Do not reuse
    - Nobody shares accounts or credentials

How to lessen vulnerabilities and risk

- Operate securely
  - Update/patch operating system software
  - Update/patch application software
  - Do not use untrustworthy software
  - Nobody should use admin accounts on regular basis
  - Develop written policies for employees to follow
  - Conduct background checks

How to lessen vulnerabilities and risk

- Operate securely
  - Update/patch operating system software
  - Update/patch application software
  - Do not use untrustworthy software
  - Nobody should use admin accounts on regular basis
  - Develop written policies for employees to follow
  - Conduct background checks

How to respond to an incident

- Do not panic! (easier said than done)
- Develop an incident response (IR) plan
- Practice the plan periodically
- Determine scope
- Take notes during incident
- Depending on scope and state laws, involve law enforcement
- Notification requirements vary by state

Questions?

Andy Green
agreen57@kennesaw.edu