

# TAKING CYBERCRIME SERIOUSLY

**How Law Firms Have Been Attacked**



# **LAW FIRMS ARE JUICY TARGETS**



# SECRETS

**2011: BAY ST. HACKED  
RE: POTASH DEAL**



**STATE ESPIONAGE?**

**SHHHH...**

**Attack Methods Are Same As For \$\$\$**

A black and white photograph showing a dense, overlapping pile of various coins. The coins are scattered across the frame, with some showing distinct features like the word 'CANADA' and a maple leaf. Overlaid on this background is the word 'MONEY' in a large, bold, white, sans-serif font, centered horizontally and vertically.

# MONEY

**“SIX FIGURE LOSS” AT  
TORONTO FIRM IN 2012**



**2013: US LAW FIRM  
HACKED FOR \$336K**

# WIRE TRANSFERS + ACH TRANSFERS

Trust Accounts = \$\$\$, Payroll = \$\$\$

---

**2013: US TITLE COMPANY  
LOSES \$1.7M VIA ACH**

# **BITCOIN RANSOMWARE**

**Cryptolocker: 2013's Fun New Method**

---

## Payment for private key



Private key will be destroyed on  
**11/24/2013**  
7:36 PM

Time left  
**71 : 58 : 56**

Choose a convenient payment method and click «Next»:

Bitcoin



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **0.5 BTC** to Bitcoin address **1gVi7gzrnJEP3eZus25CYxvJTzHVKeFfH** and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)  
[Getting started with Bitcoin](#)

<< Back

Next >>



A close-up photograph of a red wooden door. The door has a brass handle and a circular lock. The word "HOW?" is written in large, white, sans-serif capital letters across the center of the image. The background is a blurred, warm-toned wall.

# HOW?



**SPEAR  
PHISHING**

**WEBSITE  
EXPLOITS**

# **SPEAR PHISHING**

**1) Email 2) Malware 3) Record keyboard**

---



**LAW FIRM  
BOOKKEEPER HACKED**

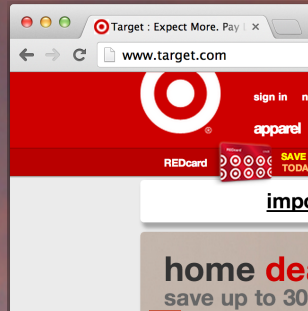
**FAKE BANK SITE +  
FAKE PHONE CALLS**

# WEBSITE EXPLOITS

1) Attack public site 2) Gain internal access

---

**TARGET: 110 MILLION  
CUSTOMERS AFFECTED**



1) Thieves break into public website

**Internal  
Server**

2) Find important internal servers

**Point of  
Sale  
Terminals**

3) Deploy exploit on POS devices

**Thief  
Server(s)**

4) Steal 110 million credit cards & PII



**70 CLASS ACTIONS  
FILED SO FAR**

# STOP KIDDING YOURSELF

You don't have better security than Target

---

# PLAINTEXT PASSWORDS

**You're as secure as the sites you use**

---





NOW WHAT?

# LEARN MORE

<http://www.cameronhuff.com/blog/security>