

# Mo' Money Mo' Problems

Making A LOT more money on  
the Web the black hat way

**Jeremiah Grossman**  
Founder & Chief Technology Officer

**Trey Ford**  
Director, Solutions Architecture

**BlackHat USA 2009**  
07.30.2009

101001001001100010100100100111101000101010101110100010101000010010100010100010101010111010010000101101  
0001110100000101 285 MILLION RECORDS WERE COMPROMISED IN 2008. 01010001011010010  
1110101010101000 01101000101010010  
0100011001011001010010000101101001001010010011100100111001011010010010010100101001010010010001110100111  
10100100101011001000010010011110100001101000001010101010110010100010101011010010001110100101101010000  
0010100101100001001010010010010100000101010011010011010101011001000110010101000100010001010111010001100  
00010010010010100010001001000010100101011010010001010101100101001011010001000101010001000100010001  
100101001111010100000101000001001011010010100101001001010000100100101010011010100110100101101001101010  
0100100101001000110010110100101010001000010010101100100001001001010010101010100011101000101010110010100  
1001001010010010010100011101001010010101000100010001000011010100000101010001011010010001000100010101001  
1010101010101010001001100010110100101000001000101010010110100100001010100010011100100100101001000010101  
01000111010101010100110101010110010001110100001001001111010011010101001001001001001100010000110101001  
10001100101001101010111010001100101101001001111010000110101001001001111010010000100010101000001010

A study conducted by the Verizon Business RISK Team

# 2009 Data Breach Investigations Report





# Jer-Jitsu

*"The embodiment of converged IT and physical security."*

*- InformationWeek*



**Director of Solutions  
Architecture**

**6 years as an  
information security  
consultant for  
Fortune 500s**

**PCI-DSS  
Curmudgeon**

**???**





WhiteHat  
SECURITY

# TechCrunch Layoff Tracker



<http://www.techcrunch.com/layoffs/>

## Plan B

### Hacker Stimulus Package

# Get Rich or Die Trying, 2008...



Four figures: Solving CAPTCHAs

Five figures: Manipulating payment systems

High five figures: Hacking Banks

Six figures: Scamming eCommerce

High Six figures: Defraud Affiliate Networks

Seven figures: Gaming the stock market



<http://www.youtube.com/watch?v=SIMF8bp5-qg>

**All still work just fine. :)**



# Im in ur webz



# crossing ur scripiz!



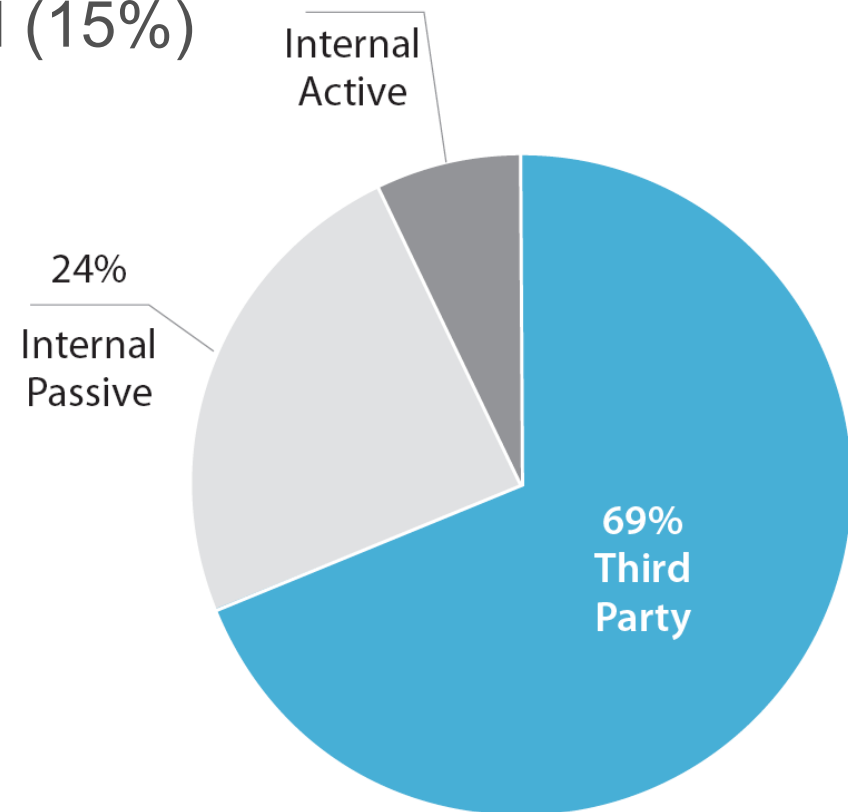
SHOW ME THE MONEY!



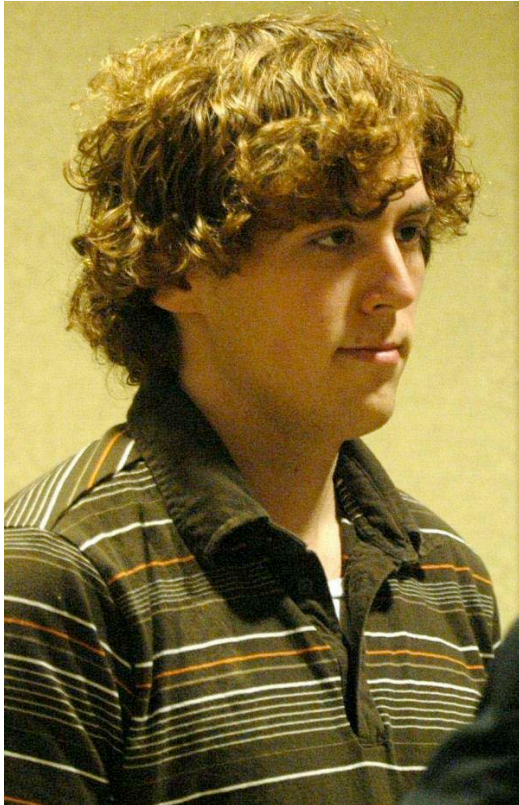
# The target won't know

## How the breach was detected:

- 3rd party detection due to FRAUD (55%)
- 3rd party detection NOT due to fraud (15%)
- Employee Discovery (13%)
- Unusual System Performance (11%)



# Don't be that guy



David Kernell, 20 year-old student University of Tennessee student, allegedly hacked into former VP candidate Sarah Palin's Yahoo Mail.



Stephen Watt, TJX hack participant which the feds call "the largest identity theft in our Nation's history." AKA (Operation Get Rich or Die Tryin)



Gary McKinnon, described as the 'UFO Hacker,' allegedly broke into United States military and NASA computers to find evidence of government-suppressed information.



# Attacker Targeting

## Random Opportunistic

- Fully automated scripts
- Unauthenticated scans
- Targets chosen indiscriminately

## Directed Opportunistic

- Commercial and Open Source Tools
- Authentication scans
- Multi-step processes (forms)

## Fully Targeted

- Customize their own tools
- Focused on business logic
- Clever and profit driven (\$\$\$)



## The Super Hacker?

# Holiday Grinch-bots

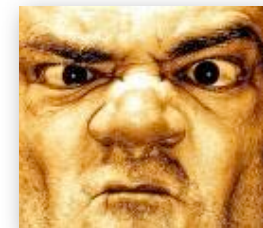
eBay's "Holiday Doorbusters" promotion, administered by Strobe Promotions, was giving away 1,000 items -- **2009 corvette, plasma TVs, jet skis, diamond ring**, etc -- to the first person to find and buy **specially-marked \$1 items**.



Some "contestants" used scripts, skipping to 'buy', without even viewing the goods. **Almost 100%** of the prizes were 'won' this way as evidenced by the **visitor counters showing "0000."**



Many were not happy and complaining in the forums. Disappointed with eBays response, some took matters into their own hands **listing "other" items for \$1**.



*"This is **picture I took of my cat** with my Cannon Powershot Camera after she overheard that people were using scripting to purchase HOLIDAY DOORBUSTERS items on eBay. **Not responsible for poor scripting techniques.**"*



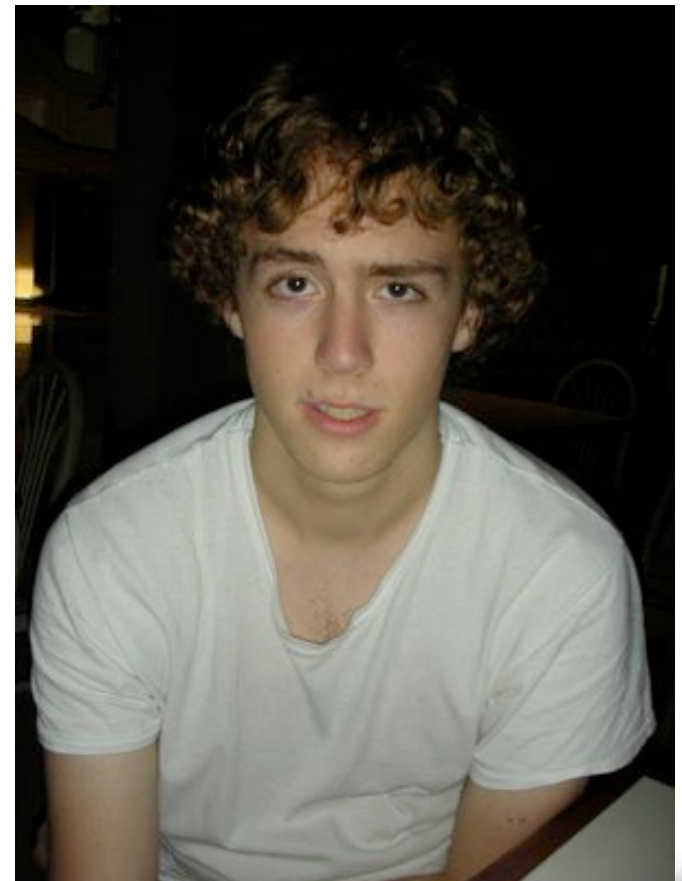
<http://redtape.msnbc.com/2008/12/ebay-users-say.html>

# Recover someone else's password - it's a feature!



?

||





# “Appropriate” access to Email

Start with just an email address



[Yahoo! Home](#) - [Help](#)

Your Progress

What did you forget?

Verify your identity

Reset your password

## Answer these questions to validate your identity

We need to verify a few questions and we'll be done.

**Birthday**

**Country of Residence**

**Postal Code**

[Exit Wizard](#)

Next

# Doing a little research

## 3. In case you forget your ID or password...

Alternate Email

Security Question

Where did you meet your spouse?

Your Answer

- Select One -

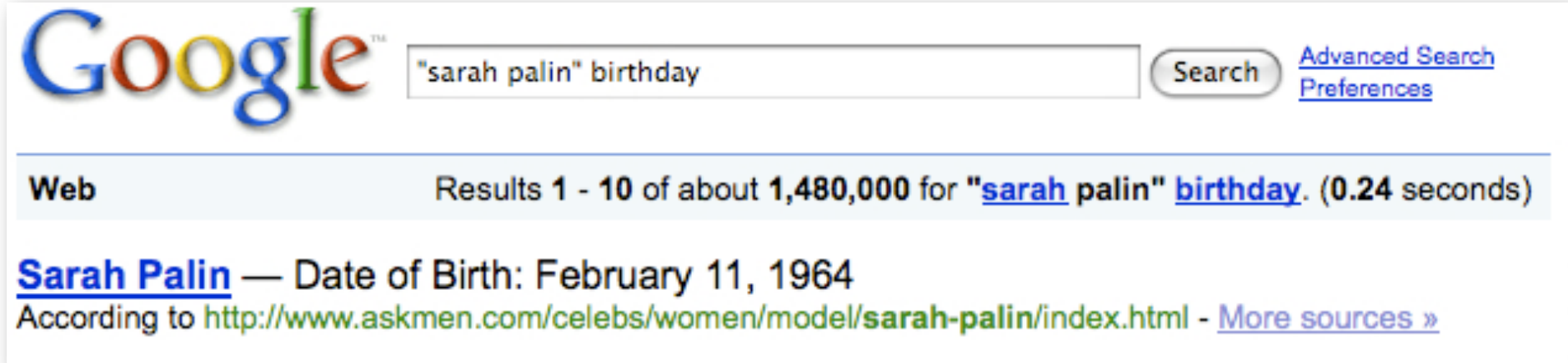
- Where did you meet your spouse?
- What was the name of your first school?
- Who was your childhood hero?
- What is your favorite pastime?
- What is your favorite sports team?
- What is your father's middle name?
- What was your high school mascot?
- What make was your first car or bike?
- What is your pet's name?

Just a couple more details...

Type the code shown



# or 'lots' of research



The image shows a screenshot of a Google search interface. The search bar contains the text "sarah palin" birthday. To the right of the search bar is a "Search" button and two links: "Advanced Search" and "Preferences". Below the search bar, the results are displayed under the heading "Web". The results show "Results 1 - 10 of about 1,480,000 for 'sarah palin' birthday. (0.24 seconds)". The first result is for "Sarah Palin" with the subtext "Date of Birth: February 11, 1964". Below this, it says "According to http://www.askmen.com/celebs/women/model/sarah-palin/index.html - More sources »".

Google™ "sarah palin" birthday Search [Advanced Search](#) [Preferences](#)

Web Results 1 - 10 of about 1,480,000 for "[sarah palin](#)" [birthday](#). (0.24 seconds)

[Sarah Palin](#) — Date of Birth: February 11, 1964  
According to <http://www.askmen.com/celebs/women/model/sarah-palin/index.html> - [More sources »](#)

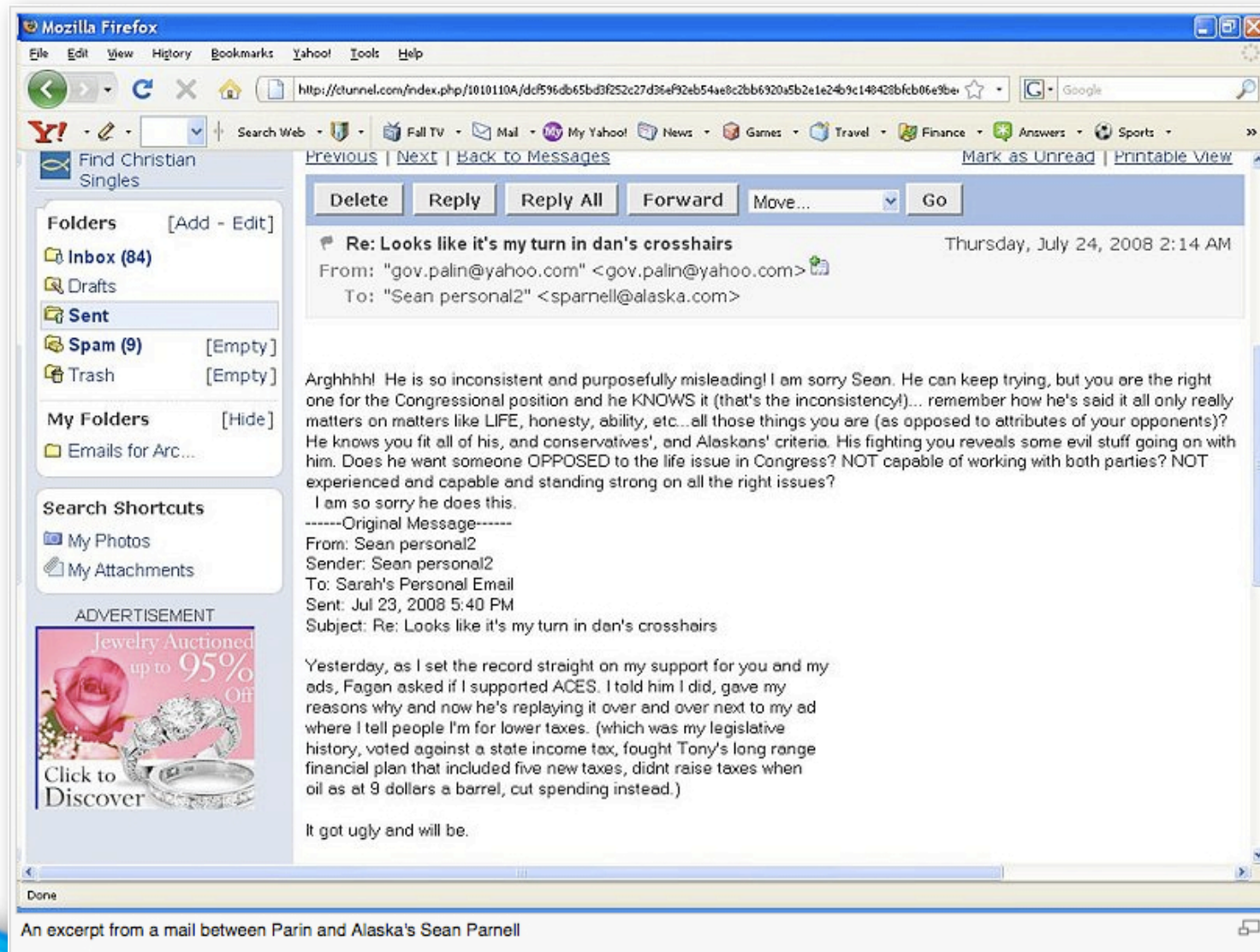
Account information used by the anonymous 'hacktivists':

```
Sarah Palin account info:  
gov.palin@yahoo.com  
DOB 2/11/64  
ZIP 99687
```

```
Todd Palin:  
fek9wnr@yahoo.com  
DOB: 9/6/64  
ZIP 99654
```



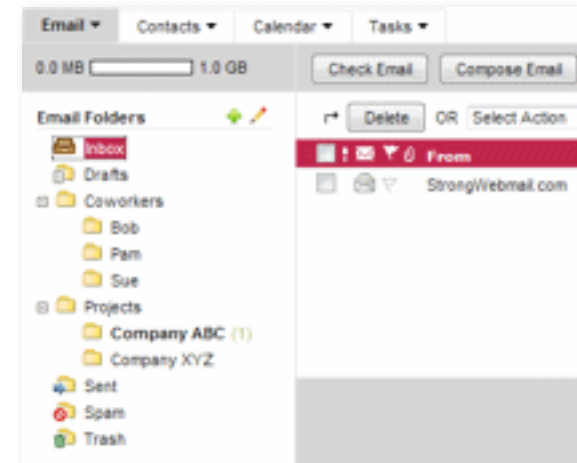
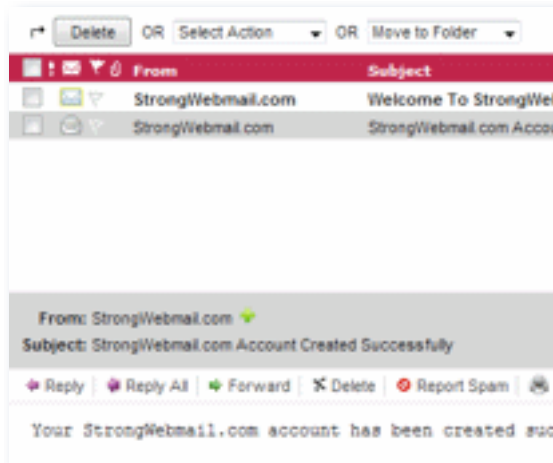
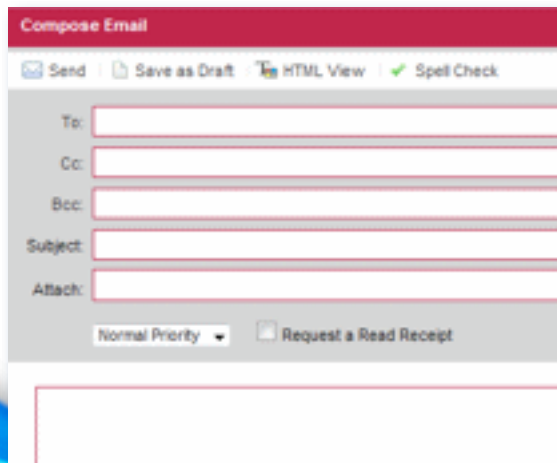
# ... and you've got MAIL



# “The most secure email accounts on the planet”



To get into a StrongWebmail account, the account owner must receive a verification call on their phone. This means that even if your password is stolen, the thief can't access your email because they don't have access to your telephone.



<http://www.strongwebmail.com/>

# Break into my email: get \$10,000. Here is my username and password.

May 21, 2009

Break into my email: get \$10,000. Here is my username and password.

Username: [CEO@StrongWebmail.com](mailto:CEO@StrongWebmail.com)

Password: Mustang85

StrongWebmail.com is offering \$10,000 to the first person that breaks into our CEO's StrongWebmail email account. And to make things easier, Strong Webmail is giving the username and password away!

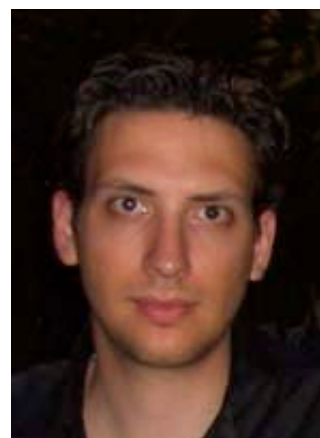
<http://www.strongwebmail.com/news/secure-web-mail/break-into-my-email-get-10000-here-is-my-username-and-password/>



# Lance James

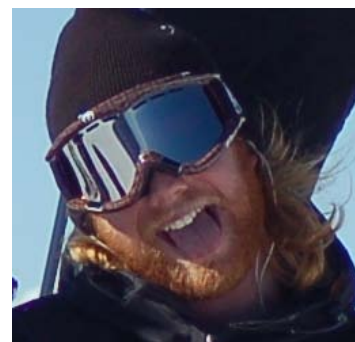


# Aviv Raff



<http://twitpwn.com/>

# Mike Bailey



<http://www.asscert.com/>

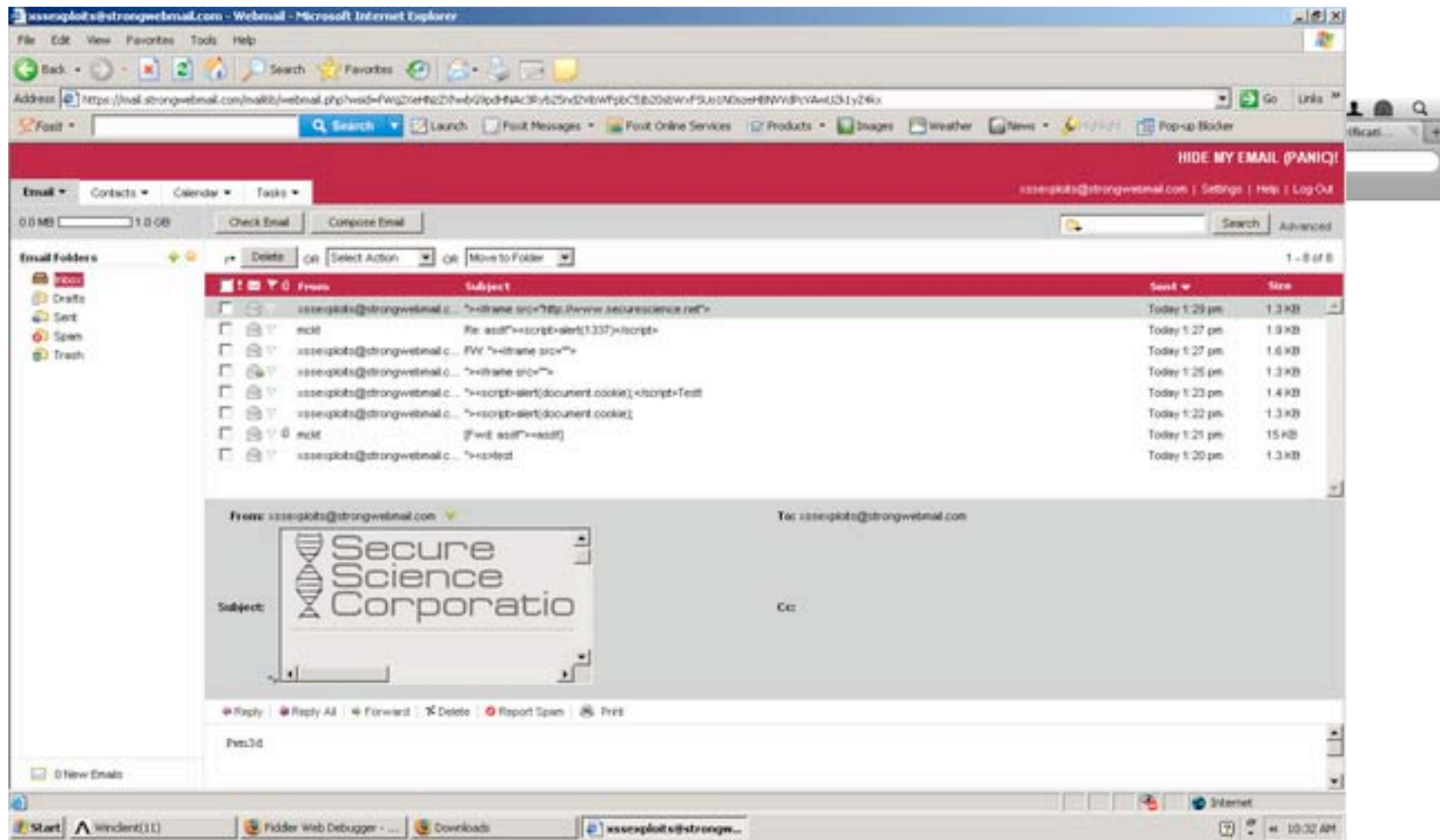
# The easiest route

- 1) Registered an account and identified multiple XSS issues in a matter of minutes (Rackspace WebMail software).
- 2) Sent ceo@strongwebmail.com an email laced with specially crafted JavaScript malware
- 3) Emailed support@strongwebmail.com stating they won the contest and sent details to the CEO encouraging them to check the account.
- 4) Within minutes the email were opened, which initiated several Ajax requests to the server, pilfering the inbox, and sending the data to a remote logging script.

<http://skeptikal.org/2009/06/strongwebmail-contest-won.html>

<http://www.fireblog.com/exclusive-interview-with-strongwebmails-10000-hacker/>

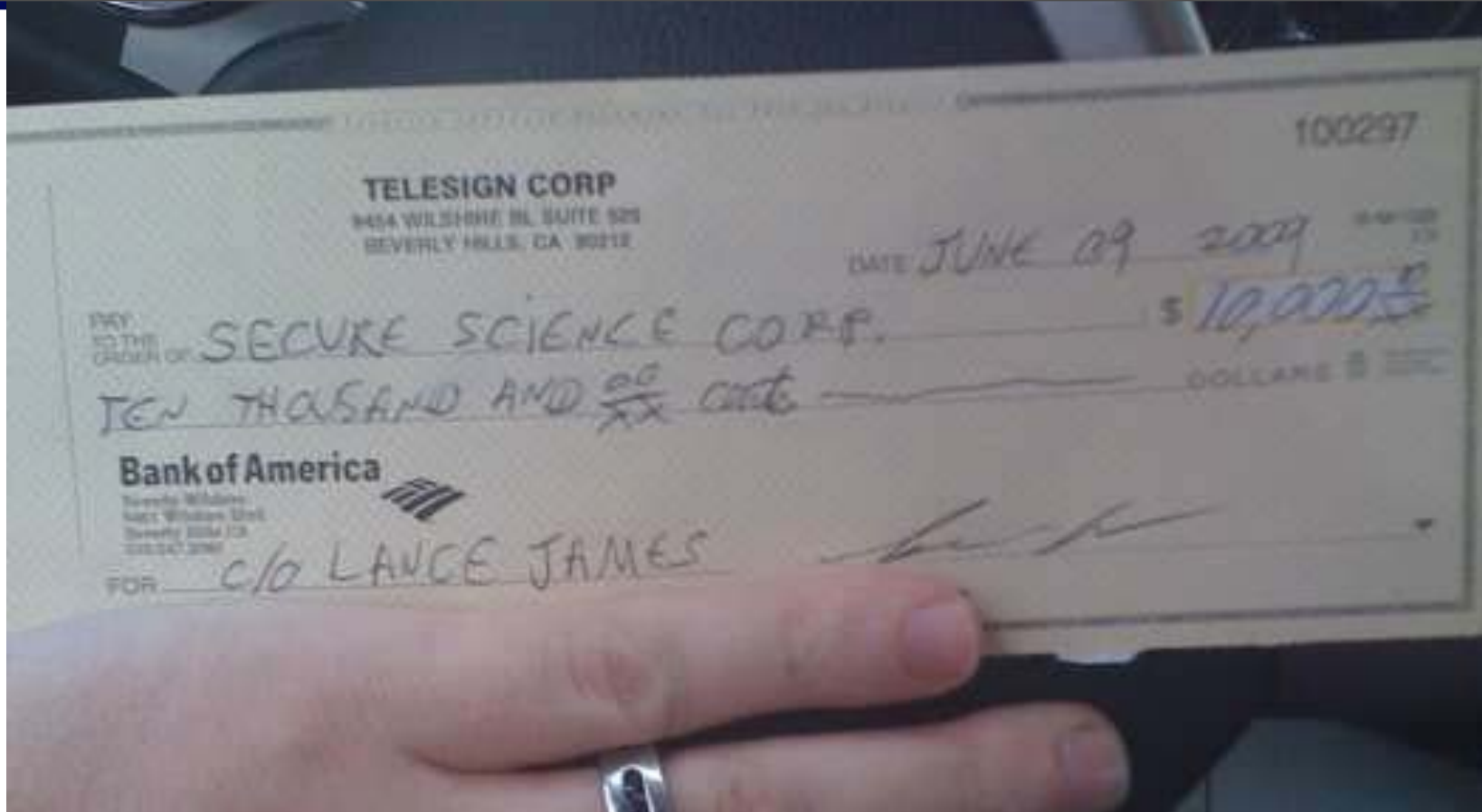
# The easiest route



Contacting "www2.teleign.com"

<http://skeptikal.org/2009/06/strongwebmail-contest-won.html>  
<http://www.fireblog.com/exclusive-interview-with-strongwebmails-10000-hacker/>





StrongWebmail said it was "not deterred" by the contest's quick conclusion and would be launching a new competition once this bug was fixed. "We won't rest until we have created the most secure e-mail in the world," the company said.

# Twitter Hacker

**Hacker Croll** initiates a password recovery for a Twitter employee's Gmail account. Reset email to secondary account: \*\*\*\*\*@h\*\*\*\*\*.com.

Guesses secondary Hotmail account, deactivated, but is able to re-register the account. Resends the reset email and bingo.

Pilfers inbox for passwords to other Web services, sets the Gmail password to the original so employee would not notice.

Used the same password to compromise employee's email on Google Apps, steal hundreds of internal documents, and access Twitter's domains at GoDaddy. **Sent to TechCrunch.**

Personal AT&T, MobileMe, Amazon, iTunes and other accounts accessed using username/passwords and password recovery systems.



*"I'm sorry" - Hacker Croll*

<http://www.techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/>

# Promo codes for cheapskates

- X% and \$X off sales
- Free Shipping
- 2 for 1 Specials
- Add-Ons & Upgrades



**NOBLEPOKER**  
NOBLEPOKER.COM

**ENTER COUPON CODE DURING SIGNUP**

Fill in your data and press the 'Create' button.

First Name:

Last Name:

Phone:

Email Address:

Currency:

Coupon Code:

[terms and conditions](#)



The collage features several coupon websites:

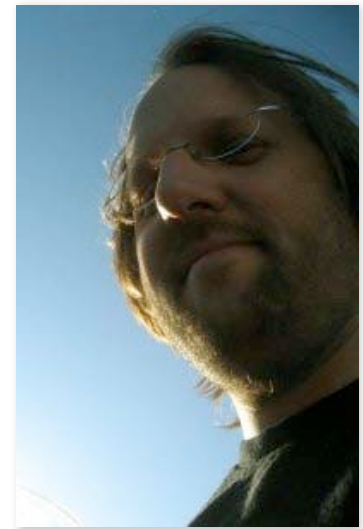
- RetailMeNot.com**: A search page for 150,000 coupon codes with a search bar and a list of categories like 'ACCESSORIES', 'BUSINESS', and 'CHILDREN'.
- Ultimate Coupons.com**: A site with a navigation menu (FATHERS DAY COUPONS, Art, Auto Parts, etc.) and a 'Featured Coupons' section listing offers from Kohl's, Home Depot, and others.
- NaughtyCodes.com**: A site with a search bar and a 'Submit a Code' button, featuring a 'It's fun to be naughty' slogan.
- CouponCabin.com**: A site with a search bar and a 'View Coupons' section listing deals from Zappos and flowers.com.



# MacWorld Hacker VIP

Client-Side Hacking

Back to Back Free MacWorld Platinum Pass  
(\$1,695)



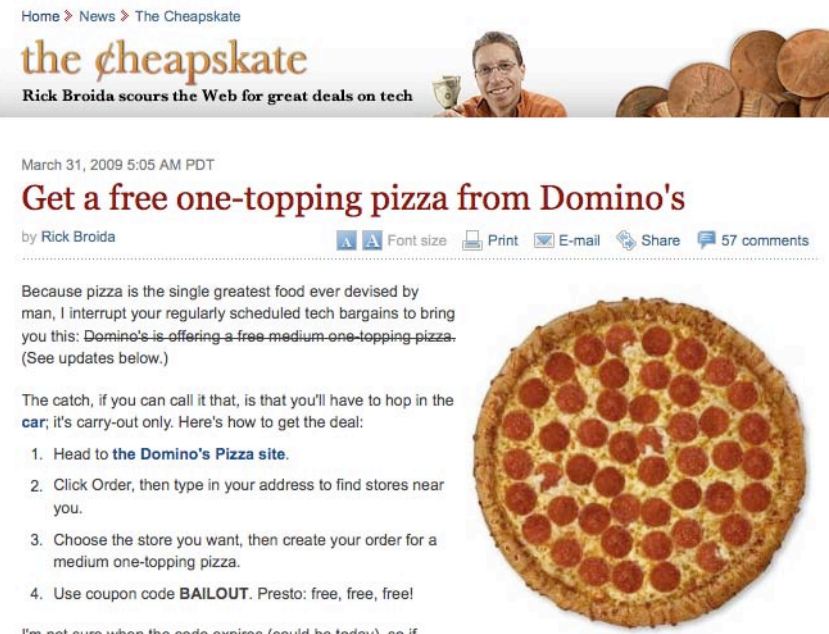
[http://grutztopia.jingojango.net/2007/01/your-free-macworld-expo-platinum-pass\\_11.htm](http://grutztopia.jingojango.net/2007/01/your-free-macworld-expo-platinum-pass_11.htm)  
<http://grutztopia.jingojango.net/2008/01/another-free-macworld-platinum-pass-yes.html>  
<http://grutztopia.jingojango.net/2008/02/your-client-side-security-sucks.html>

# Free Pizza Tastes Better

March 31, 2009...

1. Go to the Domino's Pizza site.
2. Order a medium one-topping pizza.
3. Enter coupon code **"BAILOUT"** **FREE!**

*Still have to go pick it up!*



<http://consumerist.com/5193012/dominos-accidentally-gives-away-11000-pizzas-in-bailout-promotion>  
[http://news.cnet.com/8301-13845\\_3-10207986-58.html](http://news.cnet.com/8301-13845_3-10207986-58.html)  
<http://offtopics.com/sales-coupons-promo-codes/1797-free-papa-johns-pizza-coupon-code-hack.html>



# Share the Knowledge

$$11,000 \times \$7.00 = \$77,000$$

(per pizza)

*“Spoke to a Domino's rep, who told me the free-pizza code was created internally for a promotion that was never actually green-lit.”*





# Scams that Scale

**They make money, a little or a lot.**

**Generally not considered hacking.**

**Can do them over and over again.**

# Cookie-Stuffing

Instead of using affiliate links the “traditional” way:

```
<a href="http://AffiliateNetwork/p?  
program=50&affiliate_id=100/">really cool product!</a>
```

Force affiliate requests with “Cookie Stuffing”:

```
<iframe src="http://AffiliateNetwork/p?program=50&affiliate_id=100/"  
width="0" height="0"></iframe>
```

Remove pesky referer by placing code on SSL pages:

“Clients SHOULD NOT include a Referer header field in a (non-secure) HTTP request if the referring page was transferred with a secure protocol.” - RFC 2616

Affiliate networks will get suspicious of all these requests with no referers

# Referer Manipulation

High traffic site, owned by the SEO and unknown by Affiliate network. IFRAME the site with “clean” referer.

```
<iframe src="http://niceseo/" width="0"  
height="0"></iframe>
```

Clean site, also owned by SEO, serves up cookie-stuffing code only to requests with referer of the black-hat website.

```
<iframe src="http://AffiliateNetwork/p?  
program=50&affiliate_id=100/" width="0"  
height="0"></iframe>
```

To the affiliate Affiliate network everything looks 100% legit when investigating. They will never see cookie-stuffing code. Mind the impression ratio!






# Manufacturing Links

Identify websites with a high PR or traffic, with **site:** search features, whose link results do not have “nofollow”, URLs block by robots.txt, and do not redirect.



“Powered by Google”, but others may work as well. Use a link farm to link to search results pages so they get indexed.

```
<a href="http://www.weather.com/search/websearch?Keywords=site:mysite.com+keyword&start=0&num=10&twx=on&type=web"">keyword pair</a>
```



The Weather Channel  
weather.com

Local Weather Site Web powered by Google

site:ha.ckers.org super hacker Search

Maps | Video | Photos | World | Mobile | Alerts

Bringing weather to life

Home Weather News Travel Driving Health Home & Family Sports Outdoor Activities Climate & Green On TV

Your Search: site:ha.ckers.org su...

Web Search Results 1 -10 of about 46 for site:ha.ckers.org super hacker. (.07 seconds) powered by Google

### [Remote Firefox Vulnerabilities ha.ckers.org web application ...](#)

I actually sat in a **hacker** con and watched the Errata Security guys sniff everyone's traffic ... It's **super super** easy if you know what you are looking for. ...

[ha.ckers.org/blog/20070530/remote-firefox-vulnerabilities/](#) - 20k - Cached - Similar pages

### [ha.ckers.org web application security lab](#)

... double hashed because people think they're being **super** clever, etc... < DIV STYLE="background-image: url(http://router/path.to.hack)">blah</DIV> ...

[ha.ckers.org/](#) - 45k - Cached - Similar pages

### [Token Authentication Gone Phishing ha.ckers.org web application ...](#)

**Hacker** proof? No. Yes, time based makes it harder, and I think it's ... You may have a **super**-duper algorithm or communication protocol that ...

[ha.ckers.org/blog/20060817/token-authentication-gone-phishing/](#) - 21k - Cached - Similar pages

### [SES SEO News ha.ckers.org web application security lab](#)

... there that might point the **hacker** to a more useful location to attack. ...

It just happens that both **super** good guys and **super** bad guys ...

[ha.ckers.org/blog/20060809/ses-seo-news/](#) - 8k - Cached - Similar pages

### [Looking glasses - hacking layers 2-3 via web applications ha.ckers ...](#)

So each **super**-massive-ISP sets up a script called a "looking glass" that is ...

In this way you can **hack** the 2-3 OSI layers via the web ...

[ha.ckers.org/blog/20060820/looking-glasses-hacking-layers-2-3-via-web-applications/](#) - 9k -

Cached - Similar pages

### [XSS Book ha.ckers.org web application security lab](#)

But if I'm not **super** quick on the posts and answering email, ... The Javascript then pointed to PHP script on the **hacker's** server. ...

[ha.ckers.org/blog/20070128/xss-book/](#) - 25k - Cached - Similar pages

Cheque No: [REDACTED]

Client No: [REDACTED]

Date: FEBRUARY 27, 2006

CAD .....901,733.84

Or Order

IN DOLLAR

\*\*\*\*\*

CITIBANK IRL FINANCIAL SERVICES PLC

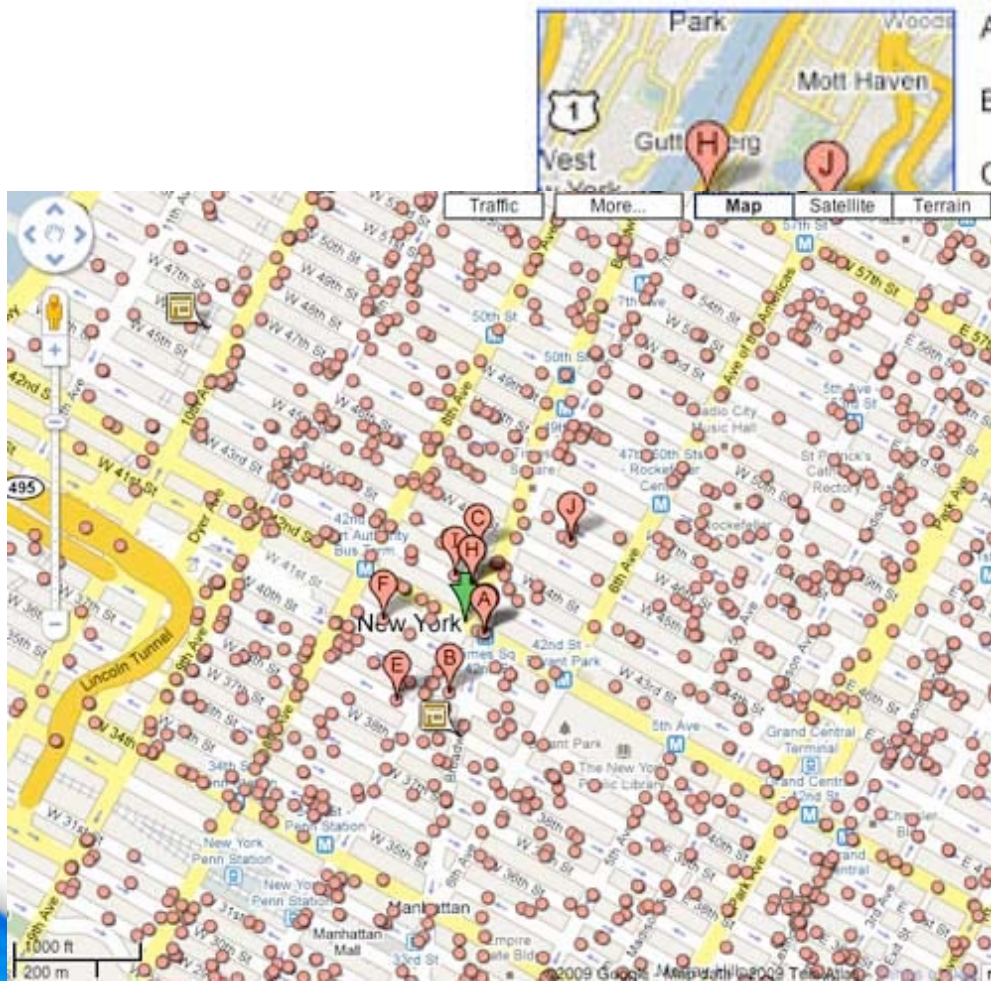
*Willen Mul*

Signature



# Google Maps vs. Spammers

## Local business results for emergency locksmith near New York, NY



- A. [Locksmith NYC \(866\) 303-3232 Emergency Locksmith 24 Hour - www.locksmith-911.com - \(866\) 620-2929 - More](#)
  - B. [New York Locksmith / Emergency \(866\) 992-8787 New York - www.locksmithservice.info - \(866\) 992-8787 - More](#)
  - C. [LOCKSMITH 866-992-8787 NEW YORK Emergency Service - www.locksmith-911.com - \(866\) 272-6287 - More](#)
  - [Locksmith NYC \(866\) 303-3232 Emergency Locksmith 24 Hour - www.24hours-locksmith.com - \(866\) 303-3232 - 1 review](#)
  - [LOCKSMITH 866-992-8787 NEW YORK Emergency Service - www.locksmith-911.com - \(866\) 697-6024 - More](#)
  - [LOCKSMITH 866-992-8787 NEW YORK Emergency Service - www.locksmith-911.com - \(866\) 282-9705 - More](#)
  - [Locksmith in NYC 866-303-3232 Emergency 24 Hours - www.24hours-locksmith.com - \(866\) 303-3232 - More](#)
  - [Locksmith 866-992-8787 New York Emergency Service - www.locksmith-911.com - \(877\) 807-6812 - More](#)
  - [LOCKSMITH 866-992-8787 NEW YORK Emergency Service - www.locksmith-911.com - \(866\) 738-0963 - More](#)
  - [Locksmith 866-992-8787 New York Emergency Service - www.locksmith-911.com - \(877\) 878-6710 - 1 review](#)
- [More results near New York, NY »](#)

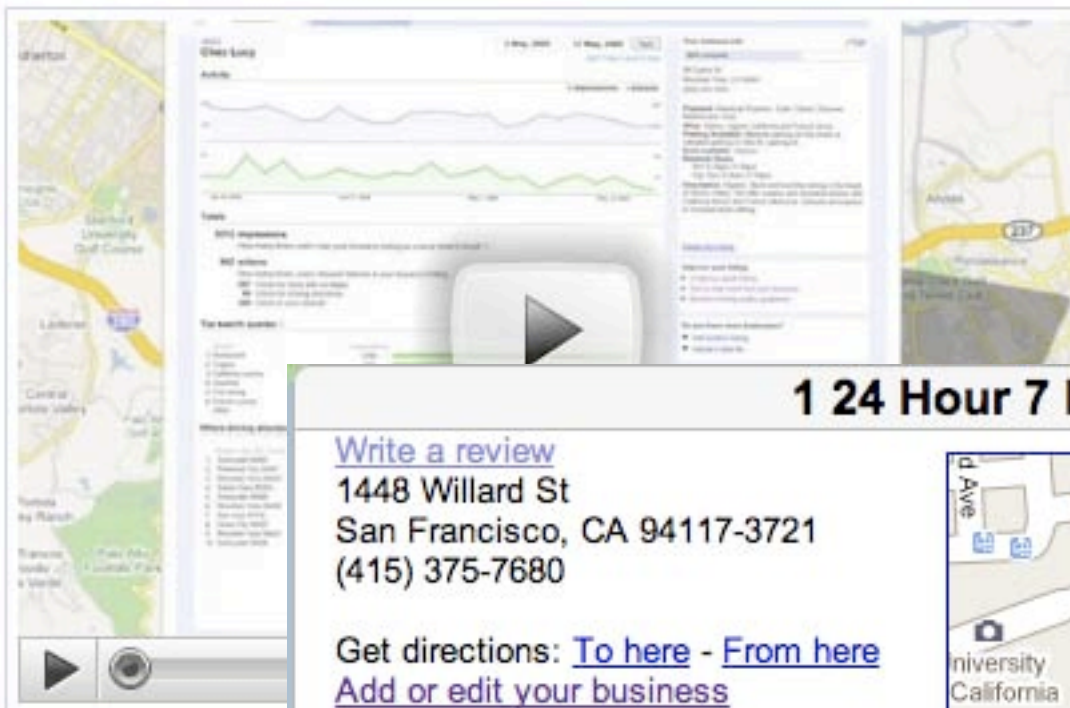
<http://blumenthals.com/blog/2009/02/25/google-maps-vs-locksmiths-spammers-spammers-winning/>  
<http://thehollytree.blogspot.com/2008/02/scam-alert-phony-israeli-owned.html>



# Google Local Business Center

# ers

**New!** Now offering a reporting dashboard. Learn how people find your business.

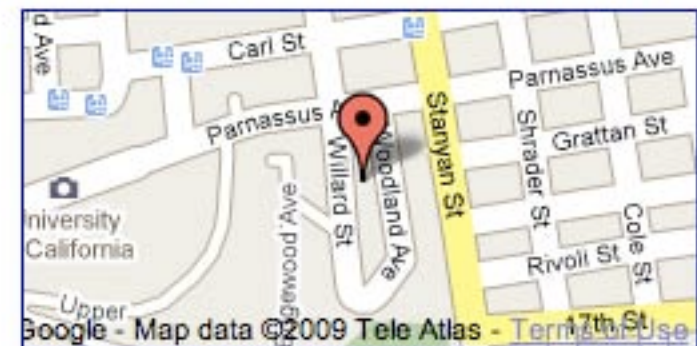


The screenshot shows a reporting dashboard with several sections: a map on the left, a central area with line graphs for 'Views' and 'Clicks', and a right-hand sidebar with various business details. A large play button is overlaid on the dashboard, indicating a video player.

**1 24 Hour 7 Day a Lock a Locksmith**

[Write a review](#)  
1448 Willard St  
San Francisco, CA 94117-3721  
(415) 375-7680

Get directions: [To here](#) - [From here](#)  
[Add or edit your business](#)



**Help customers find you on Google, it's free.**



### Free listing

Local customers already search Google for the products and services you offer. Create a business listing to be sure they find you.



### Free updates

Keep your address, phone number, hours of operation, and more up-to-date. Even create coupons and display photos and videos, all for free.

<http://bizmatters.com/blog/2009/02/25/google-maps-vs-locksmiths-spammers-spammers-winning/>  
<http://thehollytree.blogspot.com/2008/02/scam-alert-phony-israeli-owned.html>

# Google Earth Recon

Rofer Tom Berge used the aerial photographs of towns across the world to pinpoint museums, churches and schools across south London with lead roof tiles (darker colour).

Berge and his accomplices used ladders and abseiling ropes to strip the roofs and took the lead (\$164,980) in a stolen vehicle to be sold for scrap.

Sentenced to eight months in prison – suspended for two years – after confessing to over 30 offenses.



<http://www.independent.co.uk/news/uk/crime/thief-googled-163100000-lead-roofs-1645734.html>  
<http://www.telegraph.co.uk/news/uknews/4995293/Google-Earth-used-by-thief-to-pinpoint-buildings-w/valuable-lead-roofs.html>



# Returning other people's iPods

Nicholas Arthur Woodhams, 23 from Kalamazoo, Michigan set up shop online to repair iPods.



Abused Apple's Advance Replacement Program by guessing iPod serial numbers backed with Visa-branded gift cards (\$1 pre-auth).



Repeated the process 9,075 times, resold the "replacements" at heavily discounted prices (\$49), and denied any Apple credit charges.



Charged with trademark infringement, fraud, and money-laundering.



[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130136&intsrc=news\\_ts\\_head](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130136&intsrc=news_ts_head)  
[http://www.macworld.com/article/139522/23yearold\\_michigan\\_man\\_busted\\_for\\_ipod\\_fraud.html](http://www.macworld.com/article/139522/23yearold_michigan_man_busted_for_ipod_fraud.html)  
[http://www.appleinsider.com/articles/08/06/26/apple\\_makes\\_example\\_of\\_ipod\\_repairman\\_in\\_lawsuit.html](http://www.appleinsider.com/articles/08/06/26/apple_makes_example_of_ipod_repairman_in_lawsuit.html)  
<http://launderingmoney.blogspot.com/2009/03/money-laundering-charges-for-kalamazoo.html>

# Scams that scale

“Federal prosecutors have asked U.S. District Court Judge Robert Bell to let them seize real estate and personal property -- including a **2004 Audi** and a **2006 drag racer** -- as well as more than **\$571,000** in cash belonging to Woodhams, all alleged to be proceeds from his scam.”



# Jackpotting the iTunes Store

A group of U.K.-based DJs provided **19 songs**, to distributor Tunecore, who put them for sale on iTunes and Amazon.



Once online, the DJs opened accounts with **1,500 stolen or cloned US and British credit cards** to buy **\$825,000** worth of their albums **\$10** at a time over a couple month.



Apple and Amazon paid roughly **\$300,000** in royalties, which boosted their chart rankings, resulting in **even more sales and increased royalties** for the DJs.



Apple received 'stop payment' orders from credit card companies, which led to the DJs' arrest on suspicion of conspiracy to commit fraud and money laundering.



[http://www.metro.co.uk/news/article.html?DJs\\_arrested\\_in\\_%A3200,000\\_iTunes\\_scam&in\\_article\\_id=682928&in\\_page\\_id=34](http://www.metro.co.uk/news/article.html?DJs_arrested_in_%A3200,000_iTunes_scam&in_article_id=682928&in_page_id=34)



# Mythical Super Hacker

**Anyone can do this stuff!**

**Skill does not affect return on investment.**

**Competitors got caught because they didn't try not to.**

# Will Hack for \$, £, ¥, €, R\$, Rs



**HIRE HACKERS**

HOME PAGE SERVICES TUTORIALS ORDER NOW SUPPORT CONTACTS

Latest Announcements

01.12.2008  
HireHacker is discontinuing payment with Western Union & Moneygram. These two payment options are available only at client request. We do not believe in asking users to pay with a mode of payment when they have no option to get a refund in case of any issue. Client can still choose this option, but refunds are not possible in this mode.

21.11.2008  
HireHacker is now in its 5th year of existence. We've grown past expectations, survived many scares and have helped over 18,000 clients to find the truth. We thank our friends for their continuous support (and our enemies, who reminded us that we need to get better all the time).

What makes us different

HireHackers has been the most renowned password retrieval service for over 5 years. With an impeccable experience spanning over 3 years.

Welcome to HireHacker.com

**\$200 USD**  
Any Email Password  
**click to order**

Some of our Features

ONLINE SUPPORT @ 24/7/365  
We have experts available 24/7 to answer all queries. We are open 365 days.

ACCESS GUARANTEED  
If the password changes within 72 hrs after we provide it to you, we will retrieve it again for half the price.

Fixed Pricing and Charges

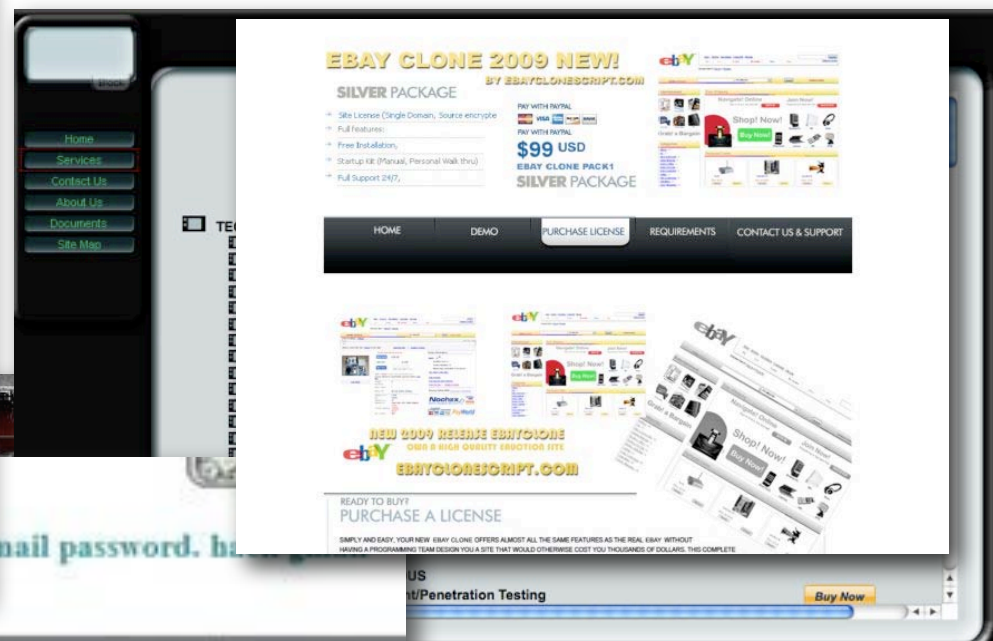
The minimum we charge for retrieving an email password is \$200 USD. Apart from a few former clients, this rule is not exceptional to anyone. Any extra bonus offered may however result in your case handled faster, on a priority basis.

Payment Options

1. Paypal (accepts creditcard)
2. Creditcard
3. Western Union
4. Moneygram

Top 10 reasons why you need us

1. Identifying Cyber Stalkers
2. Online Infidelity - Cheating Spouses
3. Employee Theft
4. Cyber harassment
5. Password Recovery
6. Internet Security Audit
7. Identity Theft
8. Online Fraud Investigations



**EBAY CLONE 2009 NEW!**  
BY EBAYCLONESCRIPT.COM

SILVER PACKAGE

- Site License (Single Domain, Source encrypted)
- Full Features
- Free Installation
- Startup 18 (18 email, Personal Walk thru)
- Full Support 24/7.

Pay With PAYPAL  
Pay With PAYPAL  
**\$99 USD**  
EBAY CLONE PACK1  
SILVER PACKAGE

HOME DEMO PURCHASE LICENSE REQUIREMENTS CONTACT US & SUPPORT

NEW 2009 RELEASE EBAYCLONE  
GIVE A HIGH QUALITY REPRODUCTION SITE

READY TO BUY?  
PURCHASE A LICENSE

SIMPLY AND EASY, YOUR NEW EBAY CLONE OFFERS ALMOST ALL THE SAME FEATURES AS THE REAL EBAY WITHOUT HAVING A PROGRAMMING TEAM DESIGN YOU A SITE THAT WOULD OTHERWISE COST YOU THOUSANDS OF DOLLARS. THIS COMPLETE

HOW IT WORKS PROOF PAYMENT OPTIONS FAQ ORDER A PASSWORD CONTACT US

WORLD LEADER IN PASSWORD RECOVERY AND SECURITY SERVICES

Hotmail	Yahoo	Rediffmail
msn Hotmail	less Yahoo in to Yahoo!	rediff.com
\$ 100 more info +	\$ 100 more info -	\$100 more info +

WE ACCEPT

e-gold  
PayPal

US  
Penetration Testing Buy Now

all Today, Sleep Tonight

online for you, and uncover the truth for you !!

Internet Spying Services  
Victims of Fraud, suspect your

**WhiteHat**  
SECURITY

... and probably are a better value for money than the  
humbly trying to present HACKING in a legal format. Instead of  
time taking it, we just CRACK the email address for you ASAP.



# Online Permit Management

In 2006, the Brazilian environment ministry did away with paper dockets and implemented an online program to issue permits documenting how much land a company could legally log and tracking the timber leaving the Amazon state of Para.



*"We've pointed out before that this method of controlling the transport of timber was subject to fraud."*

André Muggiati  
Campaigner Amazon office in Manaus  
Greenpeace International





# Amazonian Rainforest Hack

Allegedly 107 logging companies hired hackers to compromise the system, falsifying online records to increase the timber transport allocations. Police arrested 30 ring leaders. 202 people are facing prosecution.

As a result, an estimated 1.7 million cubic meters of illegal timber have been smuggled out of the Amazon, enough to fill 780 Olympic-sized swimming pools.



<http://www.greenpeace.org/international/news/hackers-help-destroy-the-amazo>

<http://www.scientificamerican.com/blog/60-second-science/post.cfm?id=hackers-help-loggers-illegally-stri-2008-12-16>

# \$833,000,000

Same computer system is used in  
two other Brazilian states.

<http://www.greenpeace.org/international/news/hackers-help-destroy-the-amazo>

<http://www.scientificamerican.com/blog/60-second-science/post.cfm?id=hackers-help-loggers-illegally-stri-2008-12-16>

# Online Permit Managers

The screenshot shows the Indiana Department of Homeland Security website. The main heading is "Application for Hazardous Material Transport Permit". Below the heading, there are two numbered sections:

- 1. If ready to apply online please have the following information ready:**
  - Information about the Organization, Shipment Carrier, and Shipment.
- 2. Other important information when filing the online application:**
  - Keep all the information at hand when filing, if the web application times you out you will have to re-type all the information.
  - If you have questions regarding the Online Application for Permit, please contact [Sue Senter](#), [Loré Laura D'Amico](#), or [Loré Laura D'Amico](#).
  - You will have to pay instant access and credit card fees to use the service.
  - If you experience technical difficulties using the application, please contact the assistance.

At the bottom of the page, there is a "National Threat Advisory: ELEVATED" section with a color-coded bar and a "Sign up to receive e-mail and wireless updates from DHS" button.

The screenshot shows the ESTA website. The main heading is "Welcome". Below the heading, there is a list of languages: English, Čeština, Dansk, Deutsch, Eesti, Español, Français, Íslenska, Italiano, 日本語, 한국어, Latviešu, Lietuvių, Magyar, Nederlands, Norsk, Português, Slovenčina, Slovenščina, Suomi, Svenska.

Below the language list, there is a "Welcome to the Electronic System for Travel Authorization Web Site." section. It states: "International travelers who are seeking to travel to the United States under the Visa Waiver Program are now subject to enhanced security requirements. All eligible travelers who wish to travel under the Visa Waiver Program must apply for authorization using the following process:"

The process is shown in a four-step flowchart:

- Step 1: Complete Your Application**
- Step 2: Submit Your Application**
- Step 3: Receive and Record Your Application Number**
- Step 4: Receive Response to Your Application**

The screenshot shows the Maine Forest Service website. The main heading is "Open Burning Permit". Below the heading, there is a "Welcome to the Open Burning Permit Online Purchasing Service" section. It states: "The Maine Forest Service is pleased to offer citizens the option to purchase open burning permits online! Through our easy online process you will be able to purchase an open burning permit 24 hours a day, 7 days a week, providing permits are being issued at the time. Although on line burn permits can be purchased at any time and are technically valid for 48 hours after payment has been submitted, **open burning can only be conducted after 5pm and before 9am**, unless there is a steady rain or the ground is completely covered with snow.

Below the welcome message, there is a "TOWN WARDEN LOGIN" section with "User Name:" and "Password:" fields and a "Login" button. There is also a "FOREST RANGER" logo.

At the bottom of the page, there is a "Maine.gov" logo and a "rights reserved." notice.

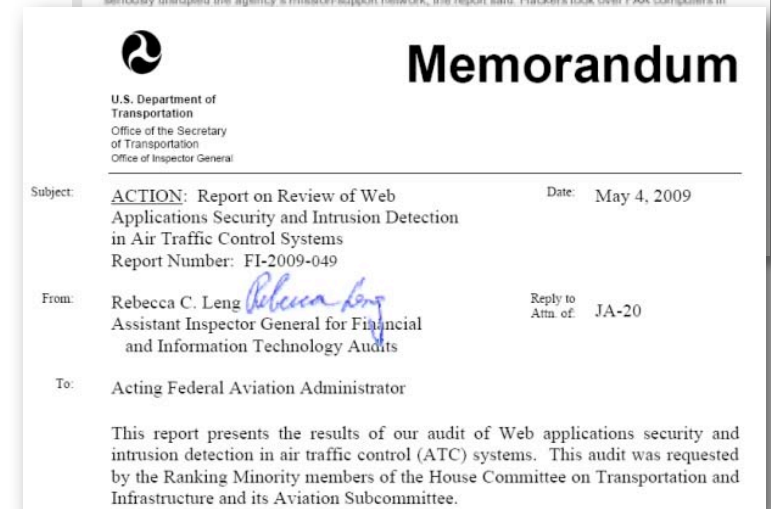


# Hiring the Good Guys



KPMG audited 70 FAA Web applications and identified 763 high-risk vulnerabilities

*“By exploiting these vulnerabilities, the public could gain unauthorized access to information stored on Web application computers. Further, through these vulnerabilities, internal FAA users (employees, contractors, industry partners, etc.) could gain unauthorized access to ATC systems because the Web applications often act as front-end interfaces (providing front-door access) to ATC systems.”*



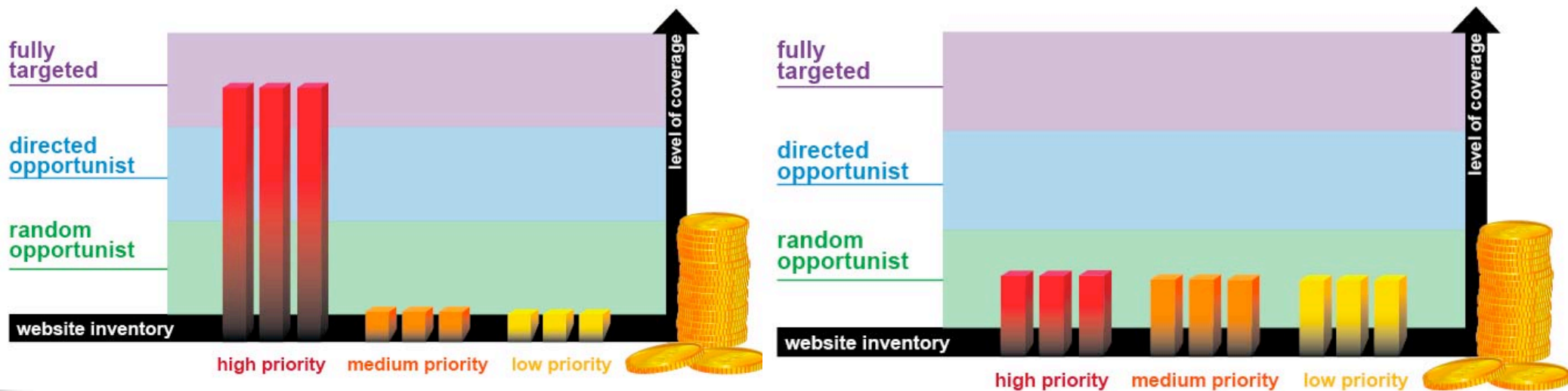
[http://news.cnet.com/8301-1009\\_3-10236028-83.html](http://news.cnet.com/8301-1009_3-10236028-83.html)  
<http://www.darkreading.com/security/government/showArticle.jhtml>  
[http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC\\_Web\\_Report.pdf](http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf)

# Security Religions

## Measure Website Security, some say...

Focus on the most important assets, test comprehensively, and get to the rest later. Defend against the **Fully Targeted** (Super Hacker). While others...

Recommend a minimum baseline for all assets, then test more thoroughly when resources allow. Defend against the **Random Opportunists** (Bots and Worms).



Success requires **FLEXIBILITY** to perform both comprehensive and scaled out testing in accordance with the organizations tolerance for risk.

# Attack Classification Misnomer

Dial is a measurement of target focus, NOT skill.

No shortage of weak websites.

Forgetting to 'not get caught'?

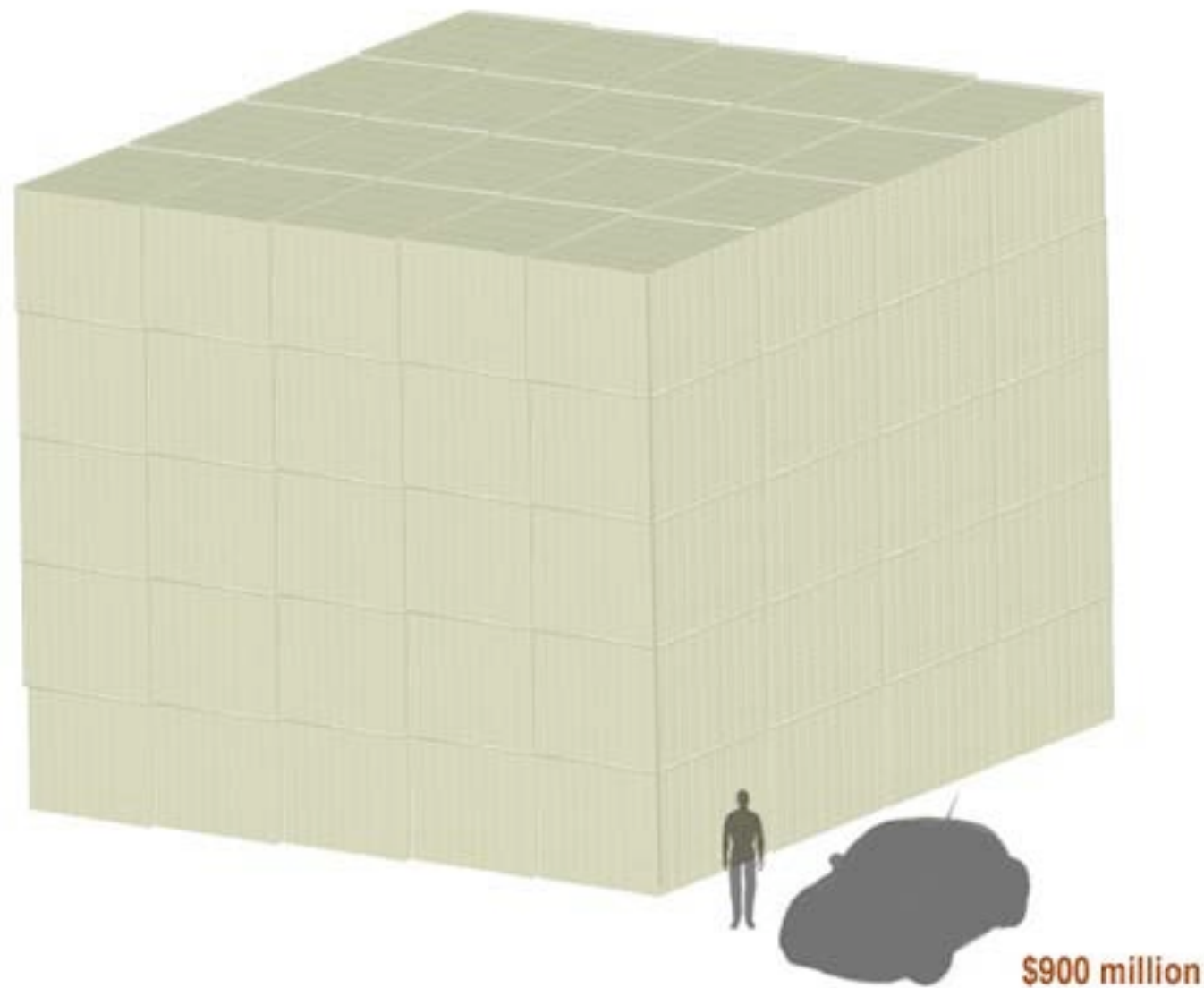
Learning 'super hacker' skillz?

Plenty of money still to be made.





# 'Plan B' Problems



# Questions?

## Jeremiah Grossman

Blog: <http://jeremiahgrossman.blogspot.com/>

Twitter: <http://twitter.com/jeremiahg>

Email: [jeremiah@whitehatsec.com](mailto:jeremiah@whitehatsec.com)

## Trey Ford

Blog: <http://treyford.wordpress.com/>

Twitter: <http://twitter.com/treyford>

[trey.ford@whitehatsec.com](mailto:trey.ford@whitehatsec.com)

## WhiteHat Security

<http://www.whitehatsec.com/>



**Link to slides  
also available**

