# Get Rich or Die Trying

*"Making money on the Web, the black hat way"*

Jeremiah Grossman
Founder & CTO

OWASP Chicago
08.21.2008



WhiteHat SECURITY

*”the embodiment of converged IT and physical security”*

Larry Greenemeier (Information Week)

WhiteHat Security
Founder & CTO

Named to InfoWorld's
CTO 25 List

Co-founder of the
Web Application
Security Consortium

Co-author of Cross-
Site Scripting Attacks

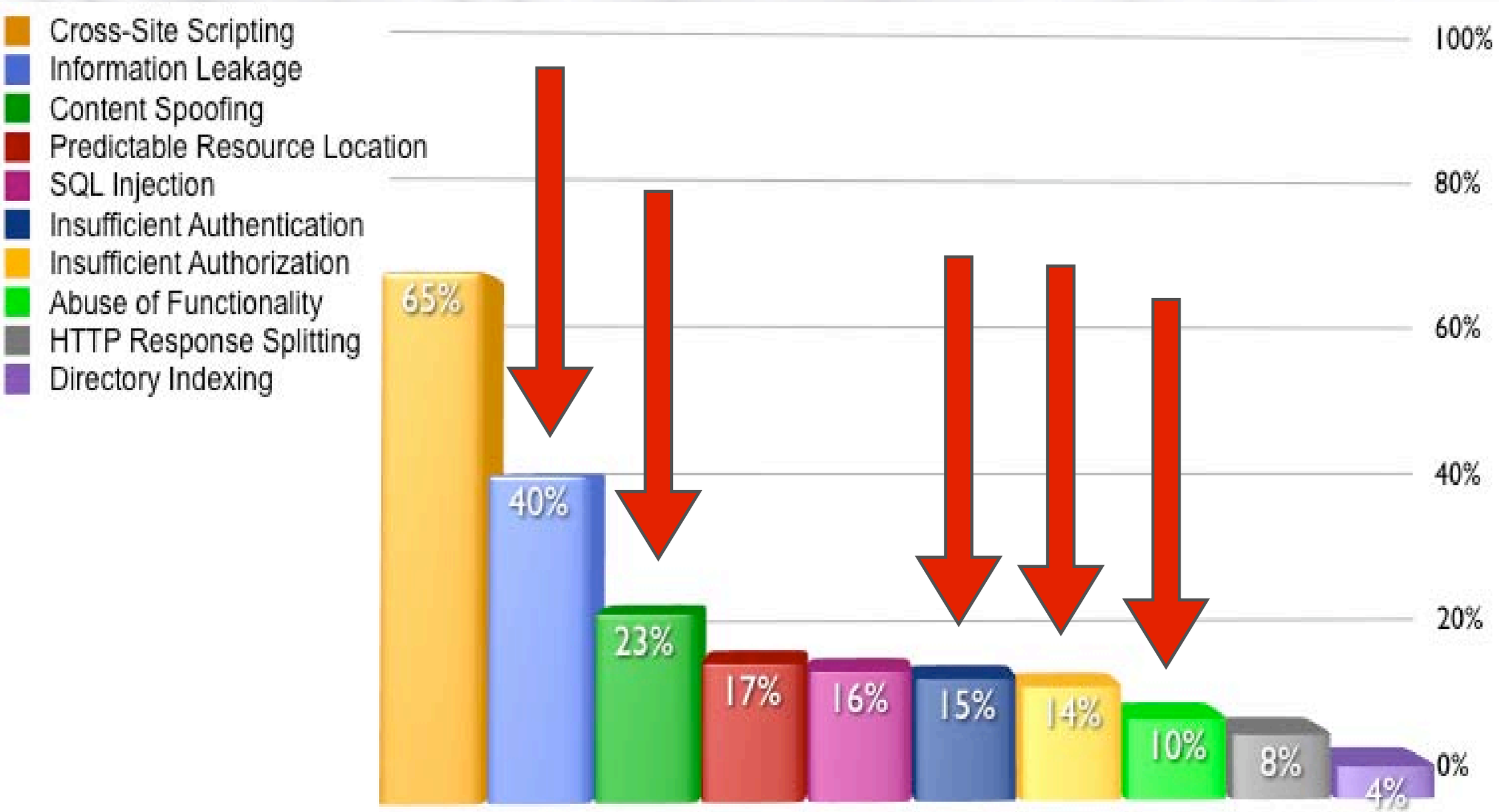
# WhiteHat Sentinel

- Unlimited Assessments – customer controlled and expert managed – the ability to scan websites no matter how big or how often they change
- Coverage – authenticated scans to identify technical vulnerabilities and custom testing to uncover business logical flaws
- Virtually Eliminate False Positives – Operations Team verifies results and assigns the appropriate severity and threat rating
- Development and QA – WhiteHat Satellite Appliance allows us to service intranet accessible systems remotely
- Improvement & Refinement – real-world scans enable fast and efficient updates




WhiteHat SECURITY

# The other half of the Top Ten




Percentage likelihood that a website has a particular vulnerability by class

# QA overlooks them

Tests what software should do, not what it can be made to do

# Scanners can't identify them

Lack intelligence and don't know if something worked (or not)

# WAFs / IDSs can't defend them

All the HTTP requests appear completely normal

# Business logic flaws = $$$

3-5 years XSS, SQLi, and CSRF probably on the way out

# Online Ballot Stuffing for Fame and Fortune

Web-based online polls are an extremely common way to capture or sway public opinion. No niche is too big or too narrow.

In response to an Austin beagle winning the Westminster Dog Show, the Austin American Statesman newspaper held on online poll (Austin's Best in Show) for Central Texas (grouped by breed). Thousands submitted photos and voted on their favorite underdogs.


*Prize: Bragging rights*

Winning the contest was all about **percentages**, not total votes...

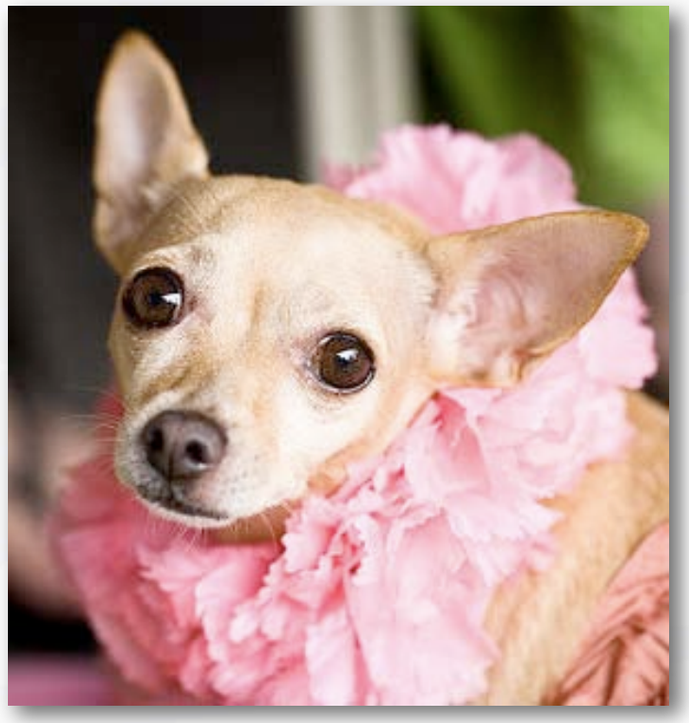
STATESMAN DOG SHOW
http://www.statesman.com/life/content/life/other/dogshow.html

# 3 ways to cheat

1. Overwhelming the positive votes
2. Overwhelming the negative votes towards competitors
3. At the last minute create a new dog and give it a positive vote - no chance of negative votes and you'll win at 100% positive.

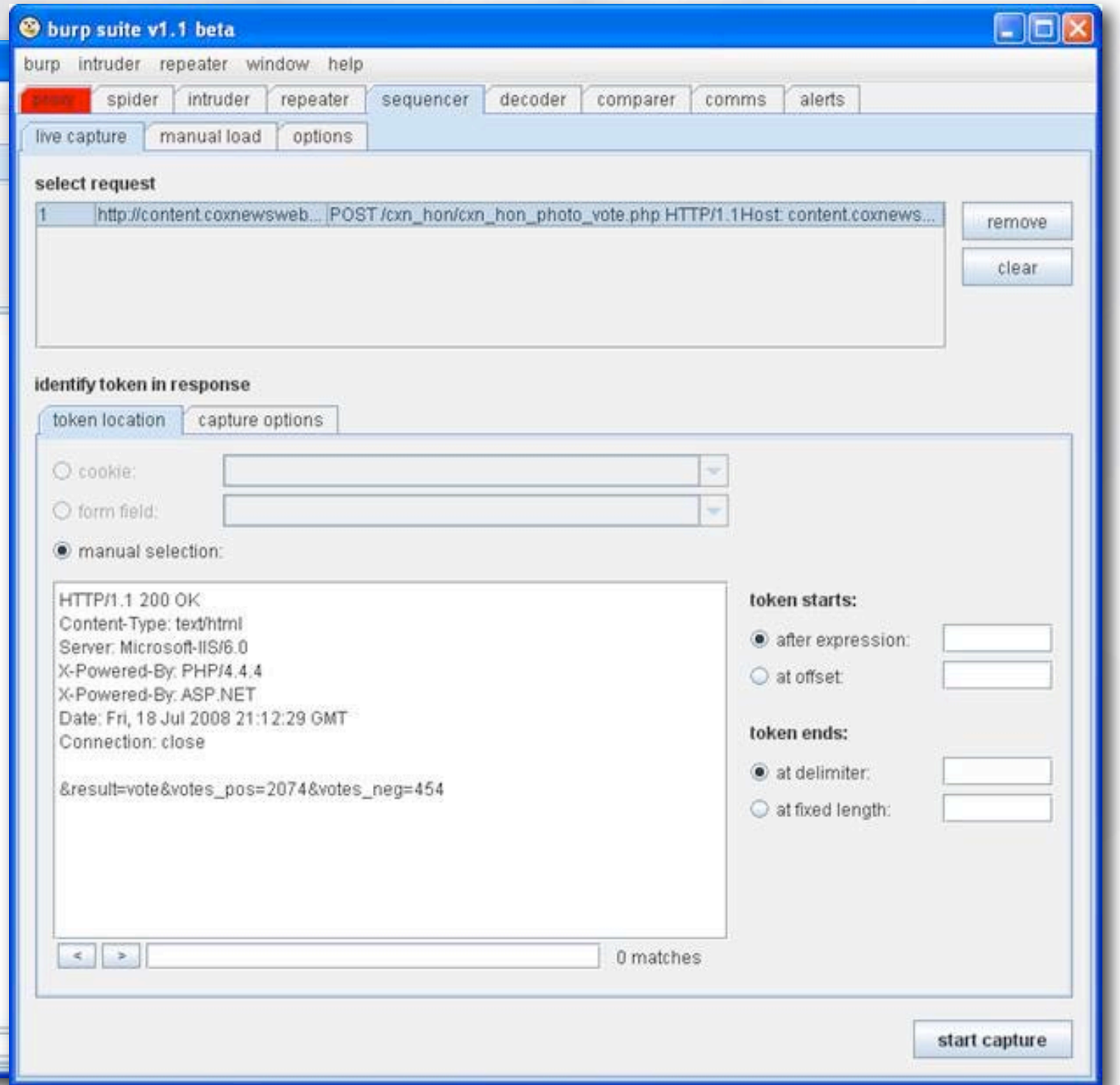
Robert “RSnake” Hansen’s girlfriend’s co-worker asks him to help her chihuahua “Tiny” win the contest.

RSnake fires up Burp proxy...



How I Lost a Contest Involving Chihuahuas
http://ha.ckers.org/blog/20080709/how-i-lost-a-contest-involving-chihuahuas/

# Taking the path of least resistance attempts #1 - submits 2,000 votes


Burp Proxy
http://portswigger.net/proxy/

# RSnake boosts Tiny into 1st...

# “ChooChoo” pwns Tiny with technique #2

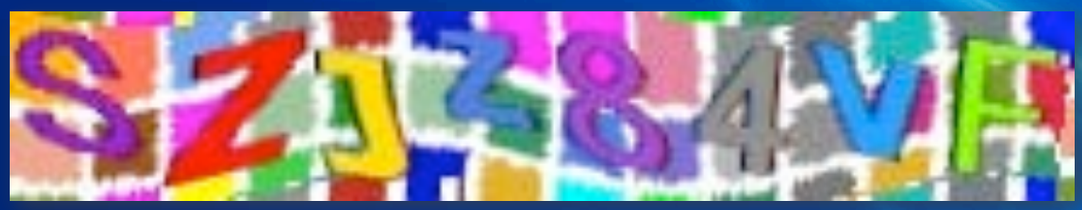
During the last minutes of the contest the competition submitted 450+ negative votes, which still made Tiny the winner in total by more than 2:1, however as a percentage of positive to negative, Tiny lost by a landslide.


FTW!

WTF!?

# Solving CAPTCHA's for Cash

Completely Automated Public Turing test to tell Computers and Humans Apart. Used for protection against bots.



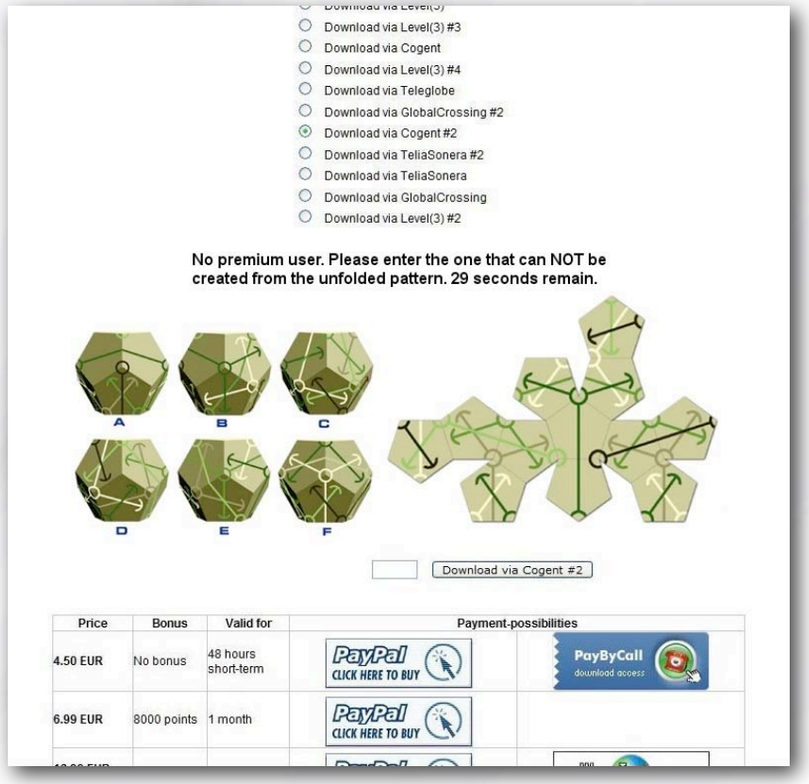
Spammers want to defeat CAPTCHAs to register for free online accounts on Gmail, YahooMail, Windows Live Mail, MySpace, FaceBook, etc. for spam distribution.

As CAPTCHA technology has become more ubiquitous a market has emerged for those who can successfully defeat the security measures in any manner possible.

**CAPTCHA solving done in 3 ways...**

# 1) Flawed Implementation

- Not enough entropy in the answers
  - i.e. “what is 4 + 1?”
- The same answers can be replayed multiple times




**CAPTCHA Effectiveness Test**

1) Test should be administered where the human and the server are remote over a network.
2) Test should be simple for humans to pass.
3) Test should be solvable by humans in less than a several seconds.
4) Test should only be solvable by the human to which it was presented.
5) Test should be hard for computer to pass
6) Knowledge of previous questions, answers, results, or combination thereof should not impact the predictability of following tests.
7) Test should not discriminate against humans with visual or hearing impairments.
8) Test should not possess a geographic, cultural, or language bias.

CAPTCHA Effectiveness Test
http://jeremiahgrossman.blogspot.com/2006/09/captcha-effectiveness-test.html
http://i32.tinypic.com/2upqp6s.jpg

# 2) OCR

**A Low-cost Attack on a Microsoft CAPTCHA**

*"Our attack has achieved a segmentation success rate of 92%, and this implies that the MSN scheme can be broken with an overall (segmentation and then recognition) success rate of more than 60%."*

**A Low-cost automated attacks on Yahoo CAPTCHAs**

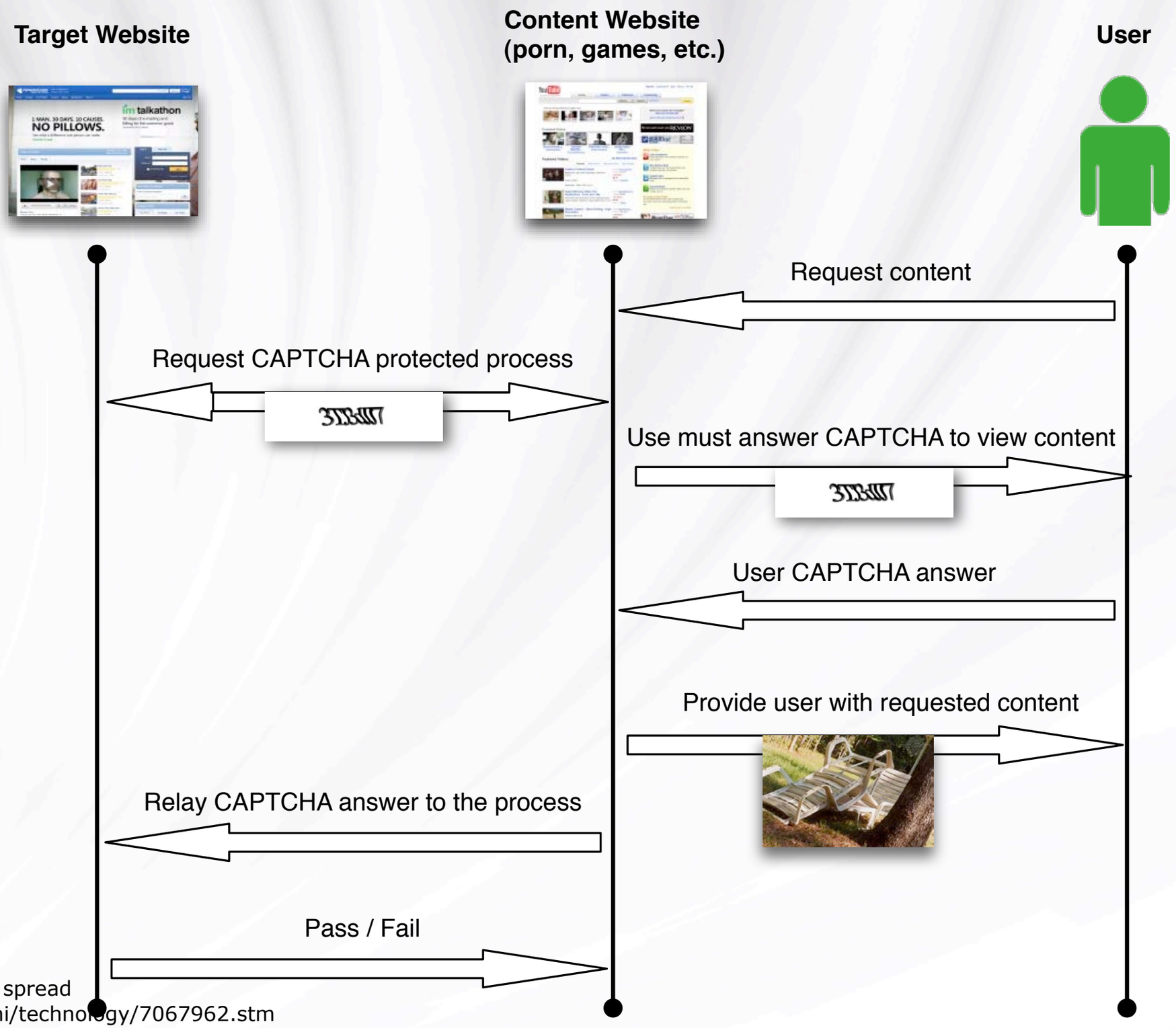
*"Our second attack achieved a segmentation success rate of around 33.4% on this latest scheme. As a result, we estimate that this scheme could be broken with an overall success rate of about 25.9%. Our results show that spammers never had to employ cheap human labour to pass Yahoo CAPTCHAs. Rather, they could rely on low-cost automated attacks. "*

*Jeff Yan and Ahmad Salah El Ahmad*
*School of Computing Science, Newcastle University, England*

Low-cost automated attacks on Yahoo CAPTCHAs
http://homepages.cs.ncl.ac.uk/jeff.yan/yahoo.htm

A Low-cost Attack on a Microsoft CAPTCHA
http://homepages.cs.ncl.ac.uk/jeff.yan/msn.htm

# 3) Mechanical Turk / “The Turk”




PC stripper helps spam to spread
http://news.bbc.co.uk/2/hi/technology/7067962.stm

Solving and creating captchas with free porn
http://www.boingboing.net/2004/01/27/solving-and-creating.html

# RSnake is contacted by a Romanian CAPTCHA Solver...

*"300-500 CAPTCHAs per person per hour. The clients pay between **$9-15 per** 1000 CAPTCHAs solved. The team works around 12 hours a day per person. That means they can solve somewhere around 4800 CAPTCHAs per day per person, and, depending on how hard the CAPTCHAs are, that can run you around **$50 per day** per person (his estimate)."*


Solving CAPTCHAs for Cash
http://ha.ckers.org/blog/20070427/solving-captchas-for-cash/

web visum (vision, in latin) is your eyes for the web
http://www.webvisum.com/

*Hello,*

*I'm from VietNam*

*We have a group with 20 person. We working some site rabot, rubl, look…*

*Our rate just **4$ for per 1000 captcha solved**.*

*We hope work you*

*Best Regard,*
*QuangHung*

*Hi!!! Hope you are doing well. We the leading Data processing company in Bangladesh. Presently we are processing 100000+ captcha per day by our 30 operators. We have a well set up and We can give the law rate for the captcha solving.*

*Our rate **$2 per 1000***
*captcha.yahoo,hotmail,mayspace,gmail, facebook etc.*

*We just wanna make the relationship for long terms. can we go forward? Thank you.*

*Best Regards*
*shakilur rahaman shohe*

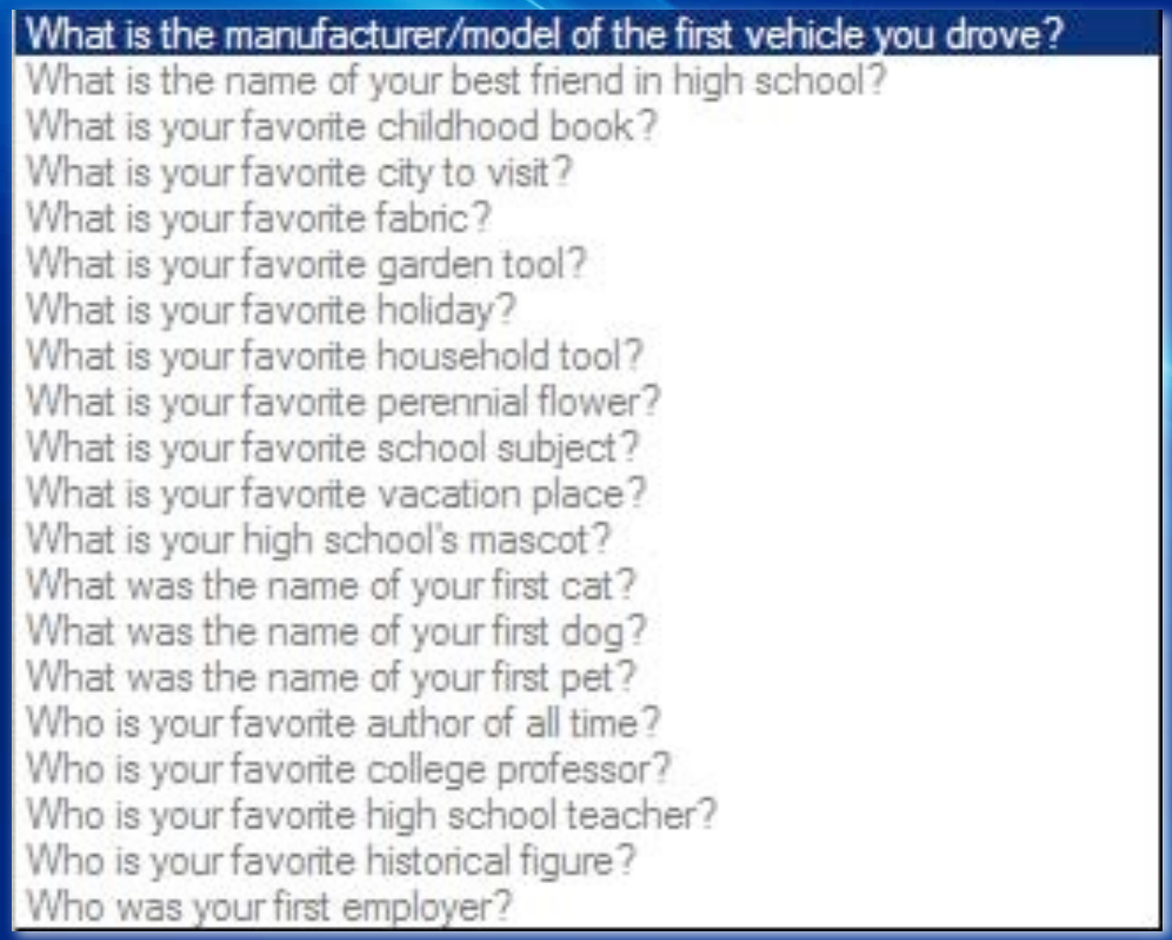
*Babu Says:*

*Dear Sir,*

*I am interested to work for data enty. Please call me 0171-3335000*

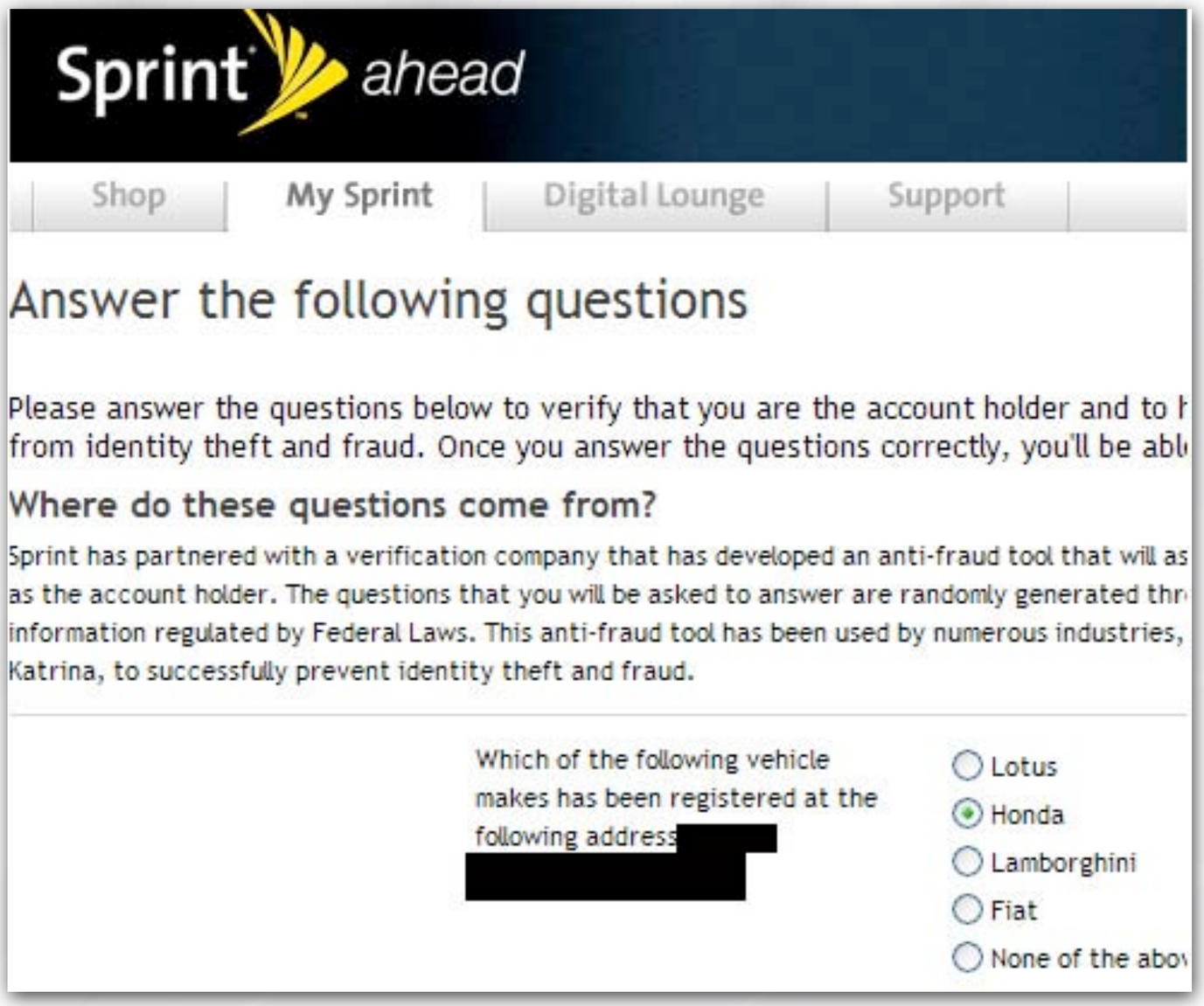
# Recover someone else's password - it's a feature!

Everyone forgets their password(s) eventually and to ease customer support costs, password recovery features are heavily relied upon.



# Hijack a Sprint user's accounts

With just a cell phone number...




*"change their billing address, order a whole bunch of cellphones sent to a drop location, and leave the victim paying the bill. There's also the stalker's wet dream: add GPS tracking to their cellphone and secretly watch their every movement from any computer."*

Flawed Security Lets Sprint Accounts Get Easily Hijacked
http://consumerist.com/tag/identity-theft/?i=376845&t=flawed-security-lets-sprint-accounts-get-easily-hijacked

# Answer the following questions

Please answer the questions below to verify that you are the account holder and to help us to protect your accoun
from identity theft and fraud. Once you answer the questions correctly, you'll be able to create your PIN.

## Where do these questions come from?

Sprint has partnered with a verification company that has developed an anti-fraud tool that will ask a short series of questions to ve
as the account holder. The questions that you will be asked to answer are randomly generated through the use of publicly available i
information regulated by Federal Laws. This anti-fraud tool has been used by numerous industries, as well as the Federal Government
Katrina, to successfully prevent identity theft and fraud.

Which of the following vehicle makes has been registered at the following address [redacted]

- ○ Lotus
- ◉ Honda
- ○ Lamborghini
- ○ Fiat
- ○ None of the above

Which of the following people have resided with you or used the same address as you at [redacted]

- ○ Jerry Stefl Iii
- ○ Ralph Argen
- ○ Jerome Ponicki
- ○ John Pace
- ○ None of the above

In which of the following cities have you NEVER lived or used in your address?

- ○ Longmont
- ○ North Hollywood
- ○ Genoa
- ○ Butte
- ◉ All of the above

# Change Billing Information

Signed on as [redacted] | Sign Off

Account number: [redacted] Account Administrator: [redacted]

To change your billing address or contact information, update the fields below:

If you want your billing statements sent to a different address than where the phones are used, please contact Customer Care. This may affect how you are taxed. Explanation of Taxes

*Due to billing cycles, your changes may not be reflected on your next invoice.

## Billing and Contact Information

* Indicates Required Information

Account name: [redacted]

Order Number/Attn:

* Street Address or PO Box: [redacted]

Suite, Apt. or Department:

* City: WASHING

* State: DC

* ZIP Code: 20012

* Contact phone number: 202[redacted]

* Contact name: [redacted]

Email Address:

Reset

Add a phone to share minutes

Payment past

Change Plan Add-ons

Add-ons for [redacted]

| | |
|---|---|
| Cellular Call Detail | Included |
| Unlimited Nights Weekends-7pm | Included |
| Picture Mail | $5.0 |
| America Expanded Voice Coverag | Included |

Check the options you want to add to your

| | |
|---|---|
| Mobile Locator ™ | $ |
| 1000 SMS Text Messages | |
| Sprint Family Locator Service | $9.99 |
| 300 SMS Text Messages | $5.00 |
| Unlimited SMS Text Messaging | $15.00 |

Save changes

Close

# Add-ons > Mobile Locator™

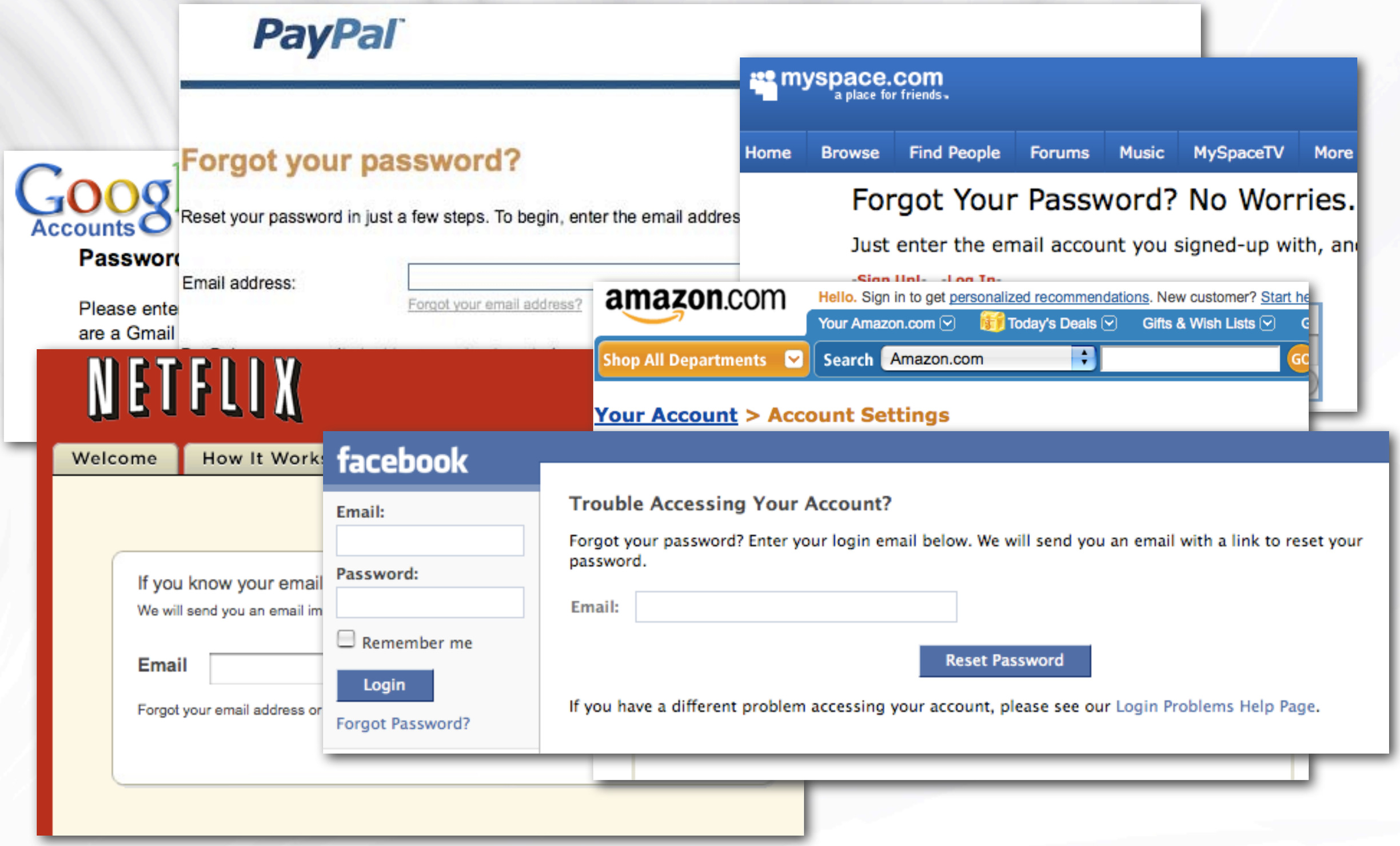
Signed on as [redacted]

< Back to the Phone & Plan landing page

## See where people are. In real time.

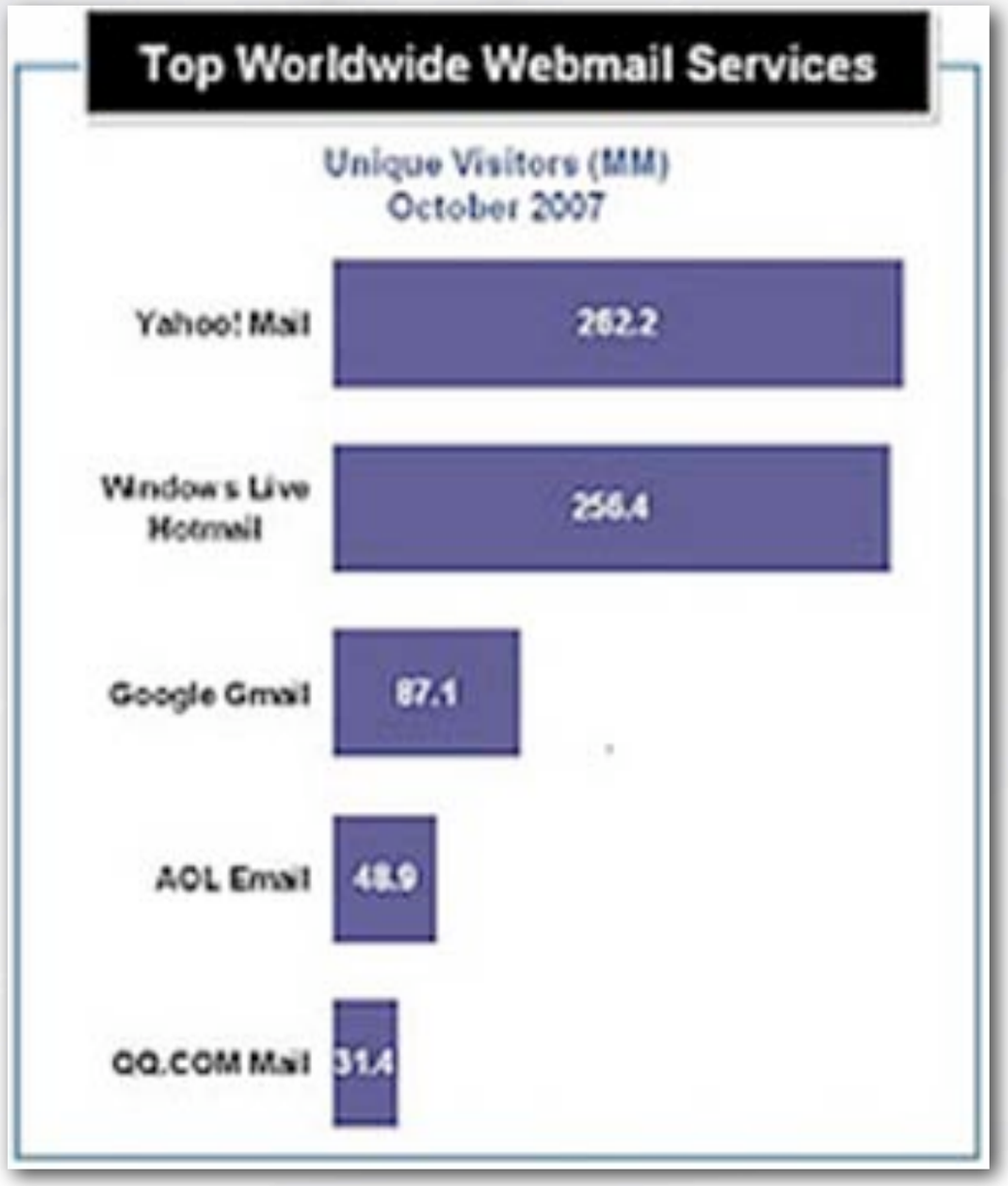
Contact Employees Anytime. Anywhere.
With Web-based Mobile Locator™ you can see the current location of an employee's phone. In real time. In the advanced mapping display on your PC. It's the information you need to provide superiro customer service, avoid delays and increase productivity. Or simply enjoy peace of mind.

# Email preferred over secret questions



# Heavy WebMail Adoption

| Provider | No. of Users (mm) |
|---|---|
| Yahoo Mail | 262.2 |
| Hotmail/Live | 256.4 |
| Gmail | 87.1 |
| AOL Mail | 48.9 |
| QQ.com | 31.4 |




Web Mail Services Market Share (Comscore, Oct 2007)
http://500hats.typepad.com/500blogs/2008/03/web-mail-serv-1.html

# China-based online “Password Recovery” services:
## You pay them to hack into “your” account.

300 Yuan ($43) to break an overseas mailbox password, with 85% probability of success.

200 Yuan ($29) to break a domestic mailbox password, with 90% probability of success.

1000 Yuan ($143) to break a company’s mailbox password (no success rate given).

Also on the menu:
passwords for 163, 126, QQ, Yahoo, Sohu, Sina, TOM, Hotmail, MSN…etc.

Mailbox passwords for sale, Chinese hacker business or scam?
http://www.thedarkvisitor.com/2008/04/mailbox-passwords-for-sale-chinese-hacker-business-or-scam/
http://news.cnnb.com.cn/system/2008/04/14/005548493.shtml


Variable project-based pricing $150 (USD) minimum. They accept Western Union.

Hire to Hack
http://www.hire2hack.net/

# Usernames are valuable too, especially when they're email addresses.

Phishers use login and password recovery screens to mine for valid email addresses using timing attacks.

Many large ecommerce portals and social networks consider valid email address disclosures a high severity issue because of how their websites operate and what it can lead to.

Unfortunately the only tool we have to fight against timing attacks is time. And time = money.

It's All About Timing - Sensepost Research
http://www.sensepost.com/research/squeeza/vegas_2007_timing.pdf

# Monetizing eCoupons

eCoupons are used during online checkout. The customer enters a unique id and a discount is applied to their order.

# A large online retailer offered an eCoupon program...

- Coupon (i.e. AmEx) worth between a couple dollars and several hundred contained 16-digit IDs where large sections were static and the rest sequential.

  3400 0000 0000 009
  3400 0000 0000 109
  3400 0000 0000 509

- Initially only 3 coupons were allowed to be applied to a single order, until the program became popular with larger orders and the restriction was removed.

- Someone developed a script trying thousands of possible valid coupon IDs. Orders of merchandise worth over **$50,000** were bought for mere dollars where 200 or more individual coupons applied.

# The problem went unnoticed until...

- A system capacity planning exercise uncovered CPU utilization during the night was spiking at 90%+, where during normal peak usage it was never that high.
- The FBI investigated, but the products were sent to a non-existent address.
- Apparently the person colluded with a mail carrier who intercepted the merchandise.

  Coupons are not currency, only a tool for marketing. Instead investigated by the Secret Service and now they face counts of mail fraud.

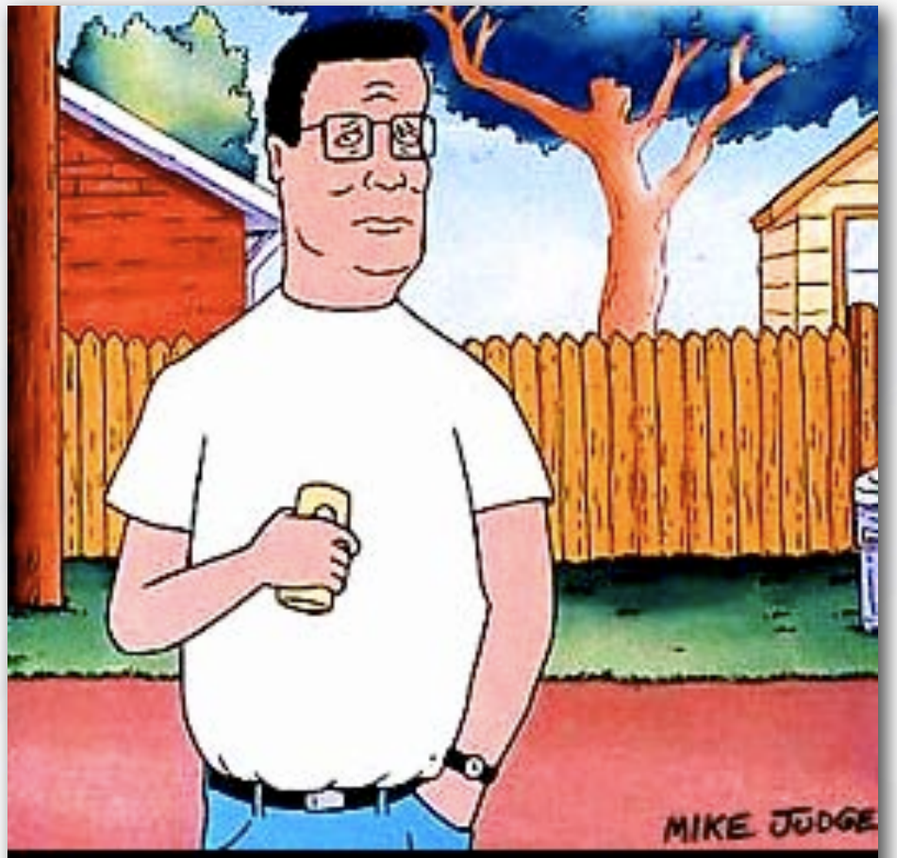
# Real life: Office Space Hack

"Micro-deposits" of a random few cents ($0.01 - $2.00) are used to verify financial accounts and routing numbers are correct and to verify that customers received it.

# Michael Largent, 22, of Plumas Lake, California allegedly...

## Opened 58,000 brokerage accounts

*"used fake names, addresses and Social Security numbers for the brokerage accounts. Largent allegedly favored cartoon characters for the names, including Johnny Blaze, King of the Hill patriarch Hank Hill, and Rusty Shackelford. That last name is doubly-fake -- it's the alias commonly used by the paranoid exterminator Dale Gribble on King of the Hill."*




Michael Largent allegedly used a script to open 58,000 online brokerage accounts in the names of cartoon characters, and other aliases.
*Hank Hill courtesy Fox Broadcasting*

## Linked to a dozen online bank accounts including Capital One, Bancorp Metabank, Greendot and Skylight.


Man Allegedly Bilks E-trade, Schwab of $50,000 by Collecting Lots of Free 'Micro-Deposits'
http://blog.wired.com/27bstroke6/2008/05/man-allegedly-b.html

Google's Checkout: $8,225

E*TRADE, Schwab: $50,225

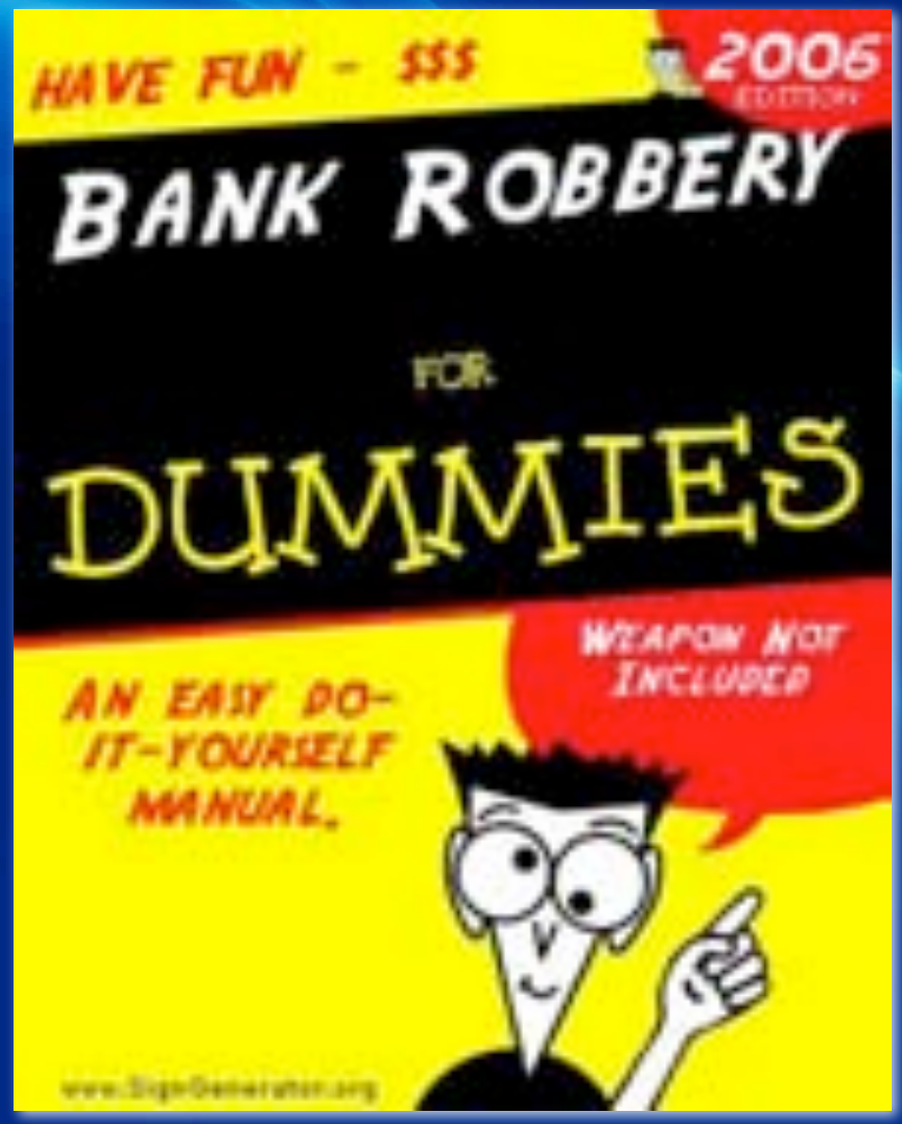
Profited using pre-paid debit cards

Faces four counts each of computer fraud, wire fraud and mail fraud.

Snared by the U.S. Patriot Act

# *“You’re a hacker!? Can you hack a bank?”*

Application Service Providers (ASP) offer hosting for banks, credit unions, and other financial services companies. ASPs are attractive targets because instead of hacking a single financial institution, an attacker could compromise dozens/hundreds/thousands.



# The System

- An ASP provides hosting for banks, credit unions, and other financial services companies. ASPs are attractive targets because **instead of focusing on one back at a time**, an attack could **compromise dozens/hundreds/ thousands at a time** with the same vulnerability.
- The banking application had three important URL parameters: **client_id, bank_id, and acct_id**. To the ASP, each of their clients has an unique ID, each potentially with several different banking websites, and each bank having any number of customer bank accounts.

http://website/app.cgi?**client_id**=10&**bank_id**=100&**acct_id**=1000

# How to hack 600 banks...

- We changed the **acct_id** to an arbitrary yet valid account #, and the error said, "**Account #X belongs to Bank #Y**"
- We then changed the **bank_id** to #Y, and an error said, "**Bank #Y belong to Client #Z**"
- We changed the **client_id** to #Z, and you could drop into anyone else's bank account, on any bank, on any client.

***Success!!!***

No notion of "authorization"
First pass at the fix *commented out the error in the HTML*, while the "real" fix would go in at some unspecified time in the future.

http://website/app.cgi?**client_id**=10&**bank_id**=100&**acct_id**=1000

# Reverse Money Transfer

**Normal: $10,000 from Account A to Account B**

A = A - ($10,000)

B = B + ($10,000)

**Negative: -$10,000 from Account A to Account B**

A = A - (-$10,000)

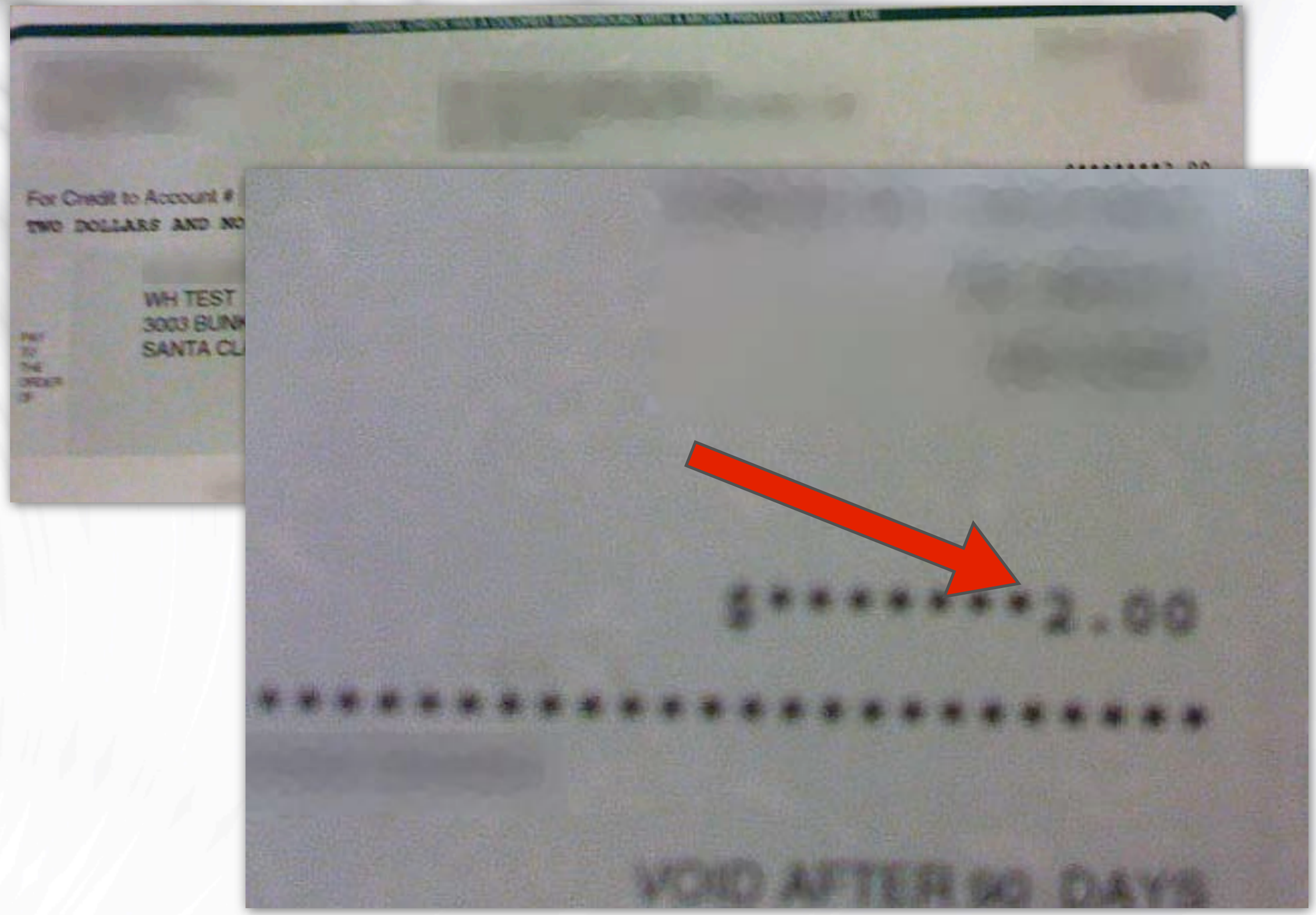
B = B + (-$10,000)

Breaking the Bank (Vulnerabilities in Numeric Processing within Financial Applications)
http://research.corsaire.com/whitepapers/technical.html

*"Back-end business controls will prevent these issues."*

*ASP Security Contact*

a few weeks later...




a couple months later...

$70,000 illegally wired to an eastern european country.

Money not recoverable.

ASP lost a customer.

Other customers affected: unknown

# When back-end order cancellation procedures are a little too slow

People order things online, then change their minds, and cancel.

Quantina Moore-Perry, 33, of Greensboro, N.C.,

Ordered (then cancelled) over 1,800 items online at QVC including handbags, housewares, jewelry and electronics


Products were shipped anyway

Auctioned off on eBay


**Profited $412,000**

Woman admits fleecing shopping network of more than $412,000
http://www.theregister.co.uk/2007/10/30/website_fraud_guilty_plea/
http://consumerist.com/consumer/crime/woman-exploited-bug-on-qvc-website-to-steal-over-400k-in-merchandise-317045.php
http://www.msnbc.msn.com/id/21534526/

"QVC became aware of the problem after being contacted by two people who bought the items, still in QVC packaging, on the online auction site."

Pleaded guilty in federal court to wire fraud.

FEDERAL TRADE COMMISSION
*PROTECTING AMERICA'S CONSUMERS*

Search >

Privacy Policy | Advanced Search | En Español

Home | News | Competition | Consumer Protection | Economics | General Counsel | Actions | Congressional | Policy

About BCP | Consumer Information | Business Information | Resources | File a Complaint

Protección del Consumidor en Español

## *Facts for Consumers*

Email | PDF Format

# Unordered Merchandise

...You respond to an advertisement offering a free "trial" pair of pantyhose. To your surprise, you receive four pair with a bill.

...You receive a pocket knife that you never ordered. Despite your objections, the company continues to send you notices demanding payment and threatening your credit rating.

What do you do when you receive merchandise that you didn't order? According to the Federal Trade Commission, you don't have to pay for it. Federal laws prohibit mailing unordered merchandise to consumers and then demanding payment.

Here are some questions and answers about dealing with unordered merchandise.

**Q. Am I obligated to return or pay for merchandise I never ordered?**

**Q. Am I obligated to return or pay for merchandise I never ordered?**

A. No. If you receive merchandise that you didn't order, you have a legal right to keep it as a free gift.

**Q. What should I do if the unordered merchandise I received was the result of an honest shipping error?**

A. Write the seller and offer to return the merchandise, provided the seller pays for postage and handling. Give the seller a specific and reasonable amount of time (say 30 days) to pick up the merchandise or arrange to have it returned at no expense to you. Tell the seller that you reserve the right to keep the merchandise or dispose of it after the specified time has passed.

**Q. Is there any merchandise that may be sent legally without my consent?**

**A.** Yes. You may receive samples that are clearly marked free, and merchandise from charitable organizations asking for contributions. You may keep such shipments as free gifts.

**Q. Is there any way to protect myself from shippers of unordered merchandise?**

**A.** When you participate in sweepstakes or order goods advertised as "free," "trial," or "unusually low priced," be cautious. Read all the fine print to determine if you are joining a "club," with regular purchasing or notification obligations.Keep a copy of the advertisement or catalog that led you to place the order, too. This may make it easier to contact the company if a problem arises.

FTC - Unordered Merchandise
http://www.ftc.gov/bcp/edu/pubs/consumer/products/pro15.shtm

# Affiliate Scams

Online merchants and advertisers enlist the services of affiliate networks to drive traffic and/or customers to their websites in exchange for a share of the revenue generate.

# The players

**Merchant**: Pays commissions to affiliates for customer clicks, account sign-ups, purchases, etc.

**Affiliate**: Collects commissions for driving customers towards merchants in the form of cost per-click (CPC) or cost per-acquisition (CPA).

**Customer**: The person who buys stuff or signs-up for promotions.

**Affiliate Network**: Technology framework connecting and monitoring the merchant, affiliate, and customer.


DarkBlue
About DarkBlue
Information Center
News & Events
Affiliates
Don't waste time arguing with Advertisers
Advertisers
We won't take a slice for ourselves
Affiliates Login
FabulousDomains
Bingo Cafe


commission junction
Commission Junction University
CJU 2008
It's selling out fast, so register today!
CLIENT LOGIN
advertisers
publishers


Google
AdSense
English (US)
Earn money from relevant ads on your website
Sign up now »
Existing AdSense users:
Sign in to Google AdSense with your
Google Account
Email
Password
Sign in
Learn about AdSense
Products
Putting ads on your site
Where do the ads come from?
Show only appropriate ads
Getting paid
How do I get started?
What our customers say


amazon.com
Join Associates
Member Sign-In
Join Associates
Explore Associates
How the Program Works
Participation is Easy and Free


eBay Partner Network
User ID
Password
GO
Make Money
by driving traffic
to eBay sites
Join the eBay Partner Network
Join Now!
How it works
Register
Advertise
Getting Paid
Optimize
Our Partner Network
Blog
Useful links

# The way it's supposed to work...

1. Affiliate signs-up with an affiliate network and places special links on their web page(s)

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

2. When users click the link their browser is sent through affiliate network where they receive a special tracking cookie and then redirected to the merchant page.

```
Set-Cookie: AffiliateID=100
```

3.If the customer buys something within X time period (i.e. affiliate cookie still exists) the affiliate receives a commission.

Using effective SEO tactics...


GOOGLE INC.
1600 AMPHITHEATRE PARKWAY
MOUNTAIN VIEW, CA 94043
Cheque No:
Client No:
Date: SEPTEMBER 27, 2005
Amount: USD **********132,994.97
Or Order
CITIBANK, N.A.
THROUGH CITIBANK (NEW YORK STATE)
ABA 0210 00868
For CITIBANK TBL FINANCIAL SERVICES PLC
Authorised Signature
ShooMoney.com

Cheque No:
Client No:

Date: SEPTEMBER 27, 2005

Amount: USD **********132,994.97

Or Order

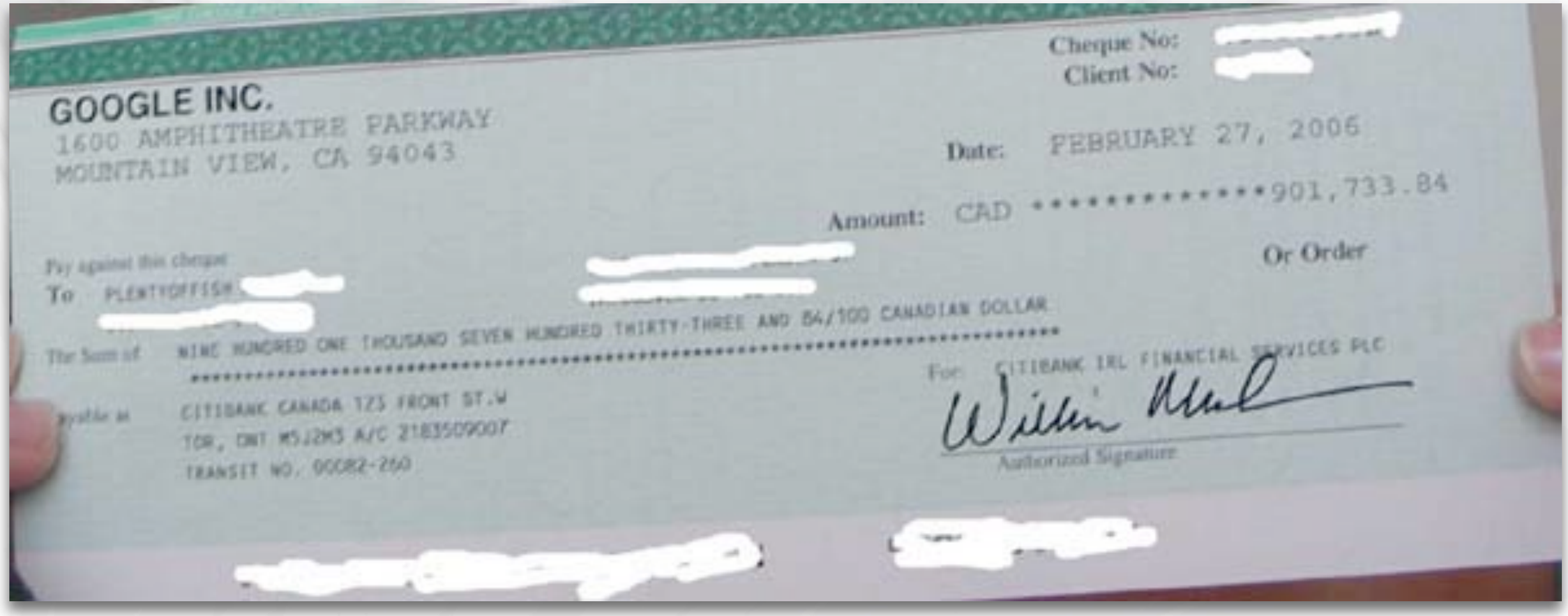
No 97/320 U.S.

**********

For CITIBANK INTERNATIONAL SERVICES PLC

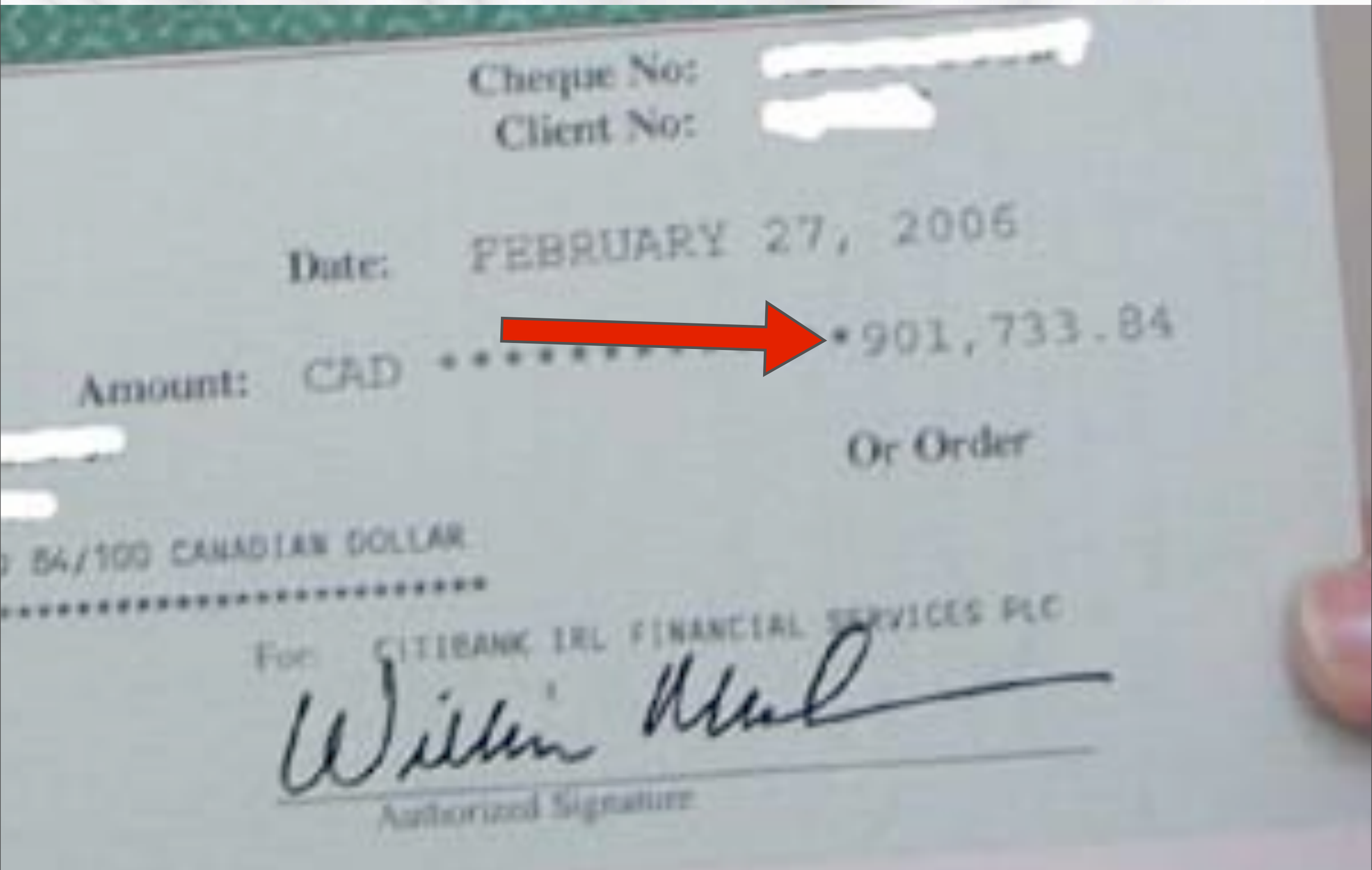
William Mark

Authorised Signature




http://hubpages.com/hub/Google_Adsense_King_-_1_Million_Dollars_Check_-_Markus_Frind_Exclusive_Interview

*"It was a check for 2 months because the first check they sent was so big it was rejected by his bank."*



# Cookie-Stuffing Circa 2002

Nothing besides pesky affiliate networks terms of service requires the user to actually “click a link” to be cookied with an affiliate ID.

Instead of:

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

Use:

```
<img src="http://AffiliateNetwork/p?program=50&affiliate_id=100/">
```

or:

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

Affiliate Programs Vulnerable to Cross-site Request Forgery Fraud
http://www.cgisecurity.org/2008/08/affiliate-progr.html

Invisible!

Aggressive affiliates figure out they can post their code anywhere online and not just on their own websites (message boards, guest books, social networks, etc).


By 2005, Merchants and Affiliate Networks got wise to cookie stuffing, start monitoring referers and conversion rates, and began kicking out suspicious affiliates.

http://www.blackhatworld.com/blackhat-seo/
http://www.gfy.com/
http://www.seoblackhat.com/forum/

# Cookie-Stuffing Circa 2007

Affiliates start posting their 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

Bottom line: No referer is sent to the affiliate to be tracked. FYI: Not every browser behaves this way, but there are many other methods to do the same using meta-refreshes and JavaScript.

**2008**: DNS-Rebinding, GIFAR, Flash malware

# Gaming customer referral incentives

1. A promotion pays affiliates $5 - $50 commission for each new user they refer who registers by submitting a new credit card number. Often it's not required that the user buy anything, perhaps only "participate".

2. Unscrupulous affiliates may register bogus accounts by the thousands with easily obtained one-time credit card numbers. The merchant or the affiliate network has no way of knowing that a credit card number is of one-time use.

3.Sources say tens of thousands to hundreds of millions of dollars have been gleaned using this method in several different marketing promotions.

# Gaming referral revenue from purchases

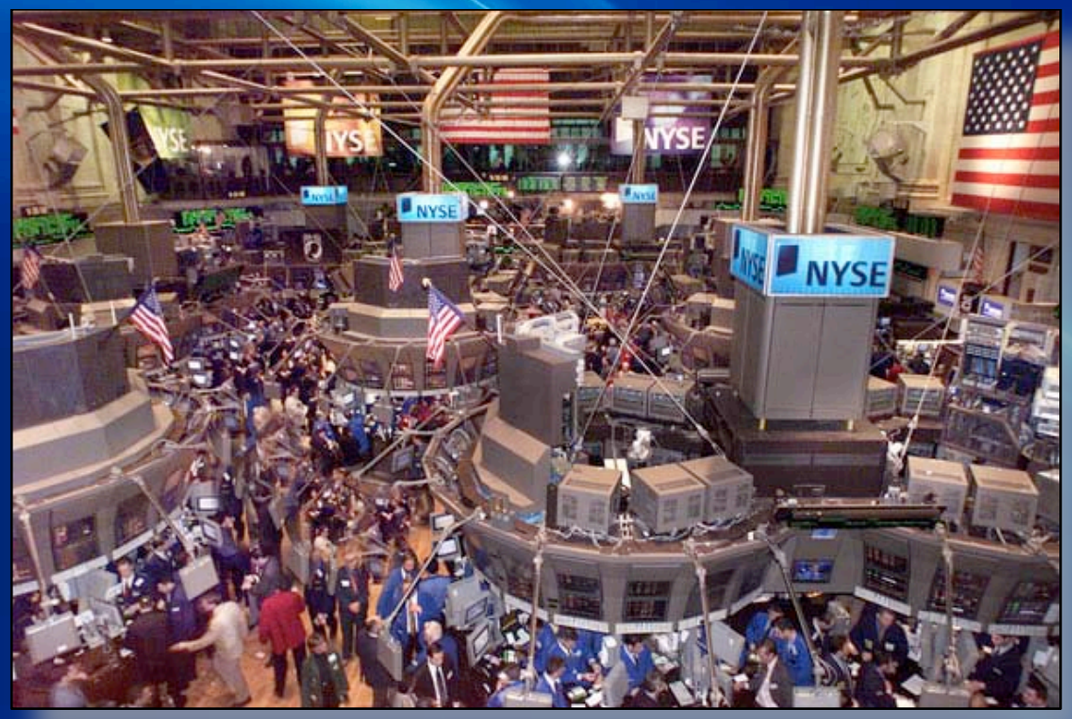
1. Merchants pay affiliates a commissions for online referral purchases.

2.Stolen credit card numbers are used to buy an item and shipped to the owner - therefore no fraud alert is issued and affiliate is paid their commission.

3. Days or weeks later the real credit card owner receives the items, reports the errors, disputes the purchase, and ships the item back. Should the merchant wish to take back their commission it is usually too late because the affiliate has been paid and long gone with the money.

# Making Millions by Trading on Semi-public Information

Insider: someone with a fiduciary role within a company. A corporate executive, investment banker or attorney. Not a hacker.



# Getting the word out...

Business Wire provides a service where registered website users receive a stream of up-to-date press releases. Press releases are funneled to Business Wire by various organizations, which are sometimes embargoed temporarily because the information may affect the value of a stock.

Press release files are uploaded to the Web server (Business Wire), *but not linked*, until the embargo is lifted. At such time, the press release Web pages are linked into the main website and users are notified with URLs similar to the following:

*http://website/press_release/08/29/2007/00001.html*
*http://website/press_release/08/29/2007/00002.html*
*http://website/press_release/08/29/2007/00003.html*

Before granting read access to the press release Web page, the system ensures the user is properly logged-in.

# Just because you can't see it doesn't mean it's not there.

An Estonian financial firm, Lohmus Haavel & Viisemann, discovered that the press release Web page URLs were named in a predictable fashion.

And, while links might not yet exist because the embargo was in place, it didn't mean a user couldn't guess at the filename and gain access to the file. This method worked because **the only security check Business Wire conducted was to ensure the user was properly logged-in, nothing more**.

According to the SEC, which began an investigation, Lohmus Haavel & Viisemann profited over **$8 million** by trading on the information they obtained.

SEC Vs. The Estonian Spiders
http://www.webpronews.com/topnews/2005/11/02/sec-vs-the-estonian-spiders

# A Ukrainian hacker breaks into Thomson Financial and steals a gloomy results announcement for IMS Health, hours before its release to the stock market ...

- Hacker enters ~$42,000 in sell orders betting the stock will fall
- The stock fell sharply making the hacker ~$300,000
- Red flags appear and the SEC freezes the funds
- Funds are ordered to be released, “Dorozhko’s alleged ‘stealing and trading’ or ‘hacking and trading’ does not amount to a violation” of securities laws, Judge Naomi Reice Buchwald
- The Times speculates that the DoJ has simply deemed the case not worth pursuing - probably due to the difficulties involved in gaining cooperation from local authorities to capture criminals in Ukraine.

Ukrainian Hacker Makes a Killing in Stock Market Fraud
http://blog.wired.com/27bstroke6/2008/02/ukrainian-hacke.html

Ukrainian hacker may get to keep profits
http://www.vnunet.com/vnunet/news/2209899/hacker-keep-profits

# Passive intelligence gathering

When online purchases are made, customers are usually provided an order tracking ID - often (semi)-sequential.

3200411
3200412
3200413

...

Pen-testers notoriously try to rotate URLs to gain access to other people's order information often containing PII:

http://foo/order_tracking?id=3200415
http://foo/order_tracking?id=3200416
http://foo/order_tracking?id=3200417
...

but we don't care about PII, only the number itself...

# The art of inference

If one could closely estimate how many “orders” a public company was on track to process at the end of a quarter, you may be able to infer (*based upon historical data*) how well they are going to do (*or how the stock price will move*).

Often these order numbers can be obtained without actually fulfilling order, OR, order then cancel.

*Hopefully the items won’t show up anyway. :)*

3200418
3200419
3200420
...

# Business logic flaws = $$$

Prime target for the bad guys

# Test often, test everywhere

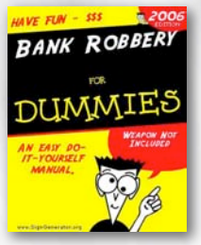
Not all vulnerabilities can be identified in the design phase, by analyzing the code, or even during QA

# Detect attacks by profiling

HTTP requests appear legitimate, but active attacks will appear anomalous

Solving CAPTCHAs - $ four figures

Manipulating payment systems - $ five figures




Hacking Banks - $ high five figures


Scamming eCommerce - $ six figures

Exploiting Affiliate Networks - $ high six figures

Gaming the stock market - $ seven figures

pwning RSnake in a chihuahua contest

***PRICELESS***

# Questions!?

For more information:  http://www.whitehatsec.com/

**Jeremiah Grossman, founder and CTO**
blog: http://jeremiahgrossman.blogspot.com/
jeremiah@whitehatsec.com



WhiteHat SECURITY