

Get Rich or Die Trying

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

Jeremiah Grossman
Founder & CTO

Arian Evans
Director of Operations

"the embodiment of converged IT and physical security"

Larry Greenemeier (Information Week)

2

A photograph of three men standing in front of a large, stylized blue and white logo on a wall. The logo features a figure in a dynamic pose, possibly a martial artist, within a shield-like shape. The man on the left is wearing a white martial arts gi with a blue belt and is making a hand gesture. The man in the center is wearing a dark blue t-shirt with a white yin-yang symbol and dark shorts. The man on the right is wearing a white martial arts gi with a blue belt and is also making a hand gesture. The background is a light-colored wall.

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

*“Who has been flirting with this subject for a few years and
is totally an 8.5+ on Hot or Not.”*

Arshan Dabirsiaghi (Author of Anti-Samy)



Director of Operations, WhiteHat Security
7 years as a enterprise security consultant
Worked with FBI, Secret Service, FinCEN, SANS, CIS, on
organized crime web hacking

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



WASC 24 Classes of Vulnerabilities

Business Logic:

Authentication

- Brute Force
- Insufficient Authentication
- Weak Password Recovery Validation

Authorization

- Credential/Session Prediction
- Insufficient Authorization
- Insufficient Session Expiration
- Session Fixation

Logical Attacks

- Abuse of Functionality
- Denial of Service
- Insufficient Anti-automation
- Insufficient Process Validation

Technical:

Command Execution

- Buffer Overflow
- Format String Attack
- LDAP Injection
- OS Commanding
- SQL Injection
- SSI Injection
- XPath Injection

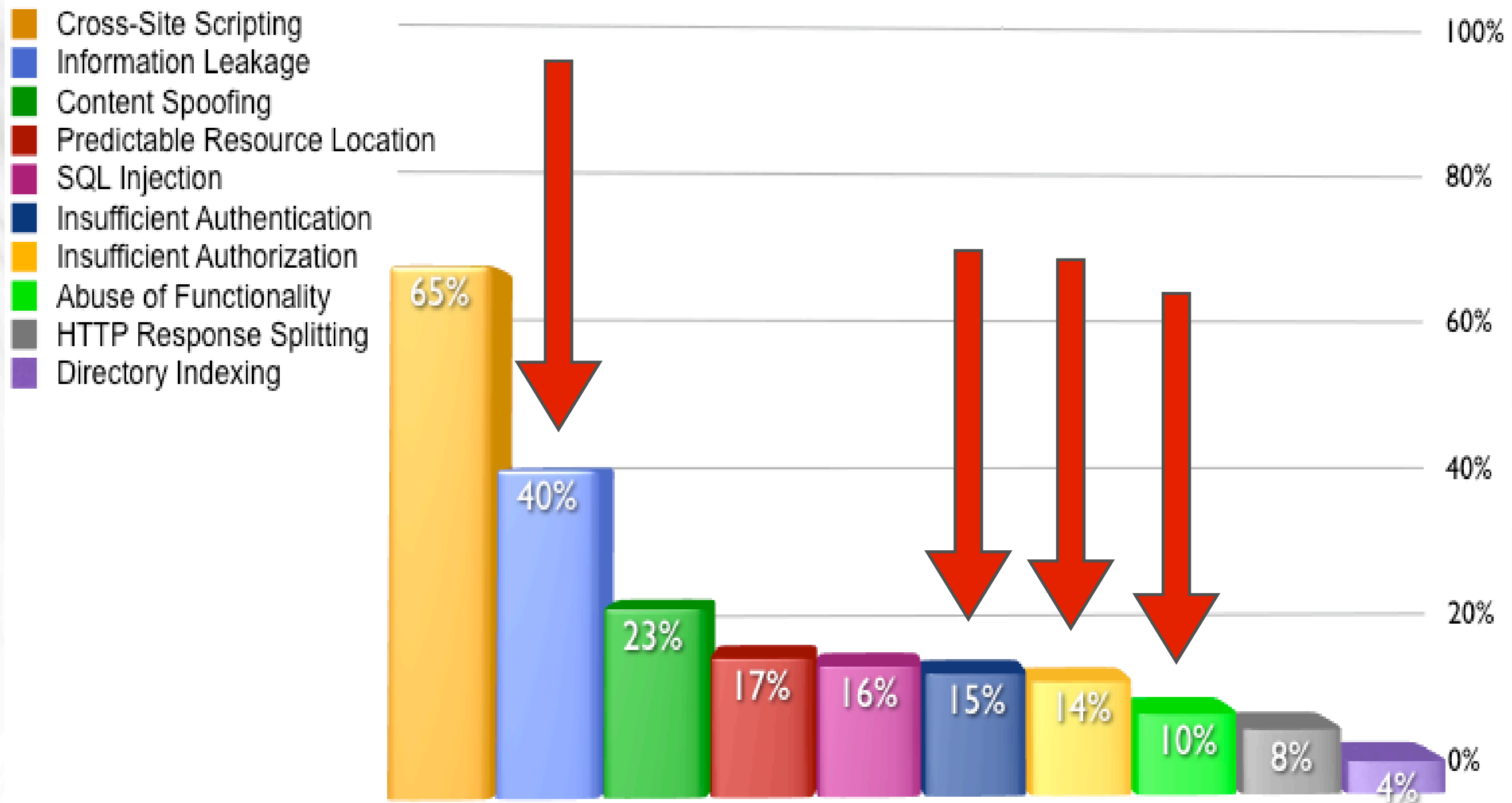
Information Disclosure

- Directory Indexing
- Information Leakage
- Path Traversal
- Predictable Resource Location

Client-Side

- Content Spoofing
- Cross-site Scripting

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

Limited contextual knowledge and doesn't know if something worked (or not)

WAFs / IDSs can't defend them

All the HTTP requests appear completely normal



Attacks are not always
“illegal” - often
just against
terms of service

Artificial Scarcity DoS

To prevent multiple-purchase of a scarce item (airline seats, physical goods, usernames, etc.), an application will “lock” the object for a period of time to prevent process conflicts.



Book an Airline Seat First, Flight Later

1. Select a flight
2. Agree to the terms and conditions
3. Provide your personal details
4. **Select seat**

***Seat is reserved and no user may select it for a variable amount of time - few minutes to several hours**

5. Enter payment information

Repeat and automate for every seat on the flight

Similar process can be applied to...

1. Event tickets (concerts, sports games, movies, conferences, etc.)

Great for scalpers who want to drive up the price on their existing tickets place or “reserve” tickets without risking a cash outlay.

2. Disrupt an eCommerce business selling a sought-after product (video games/consoles, iPhone, etc.)
3. Login Denial of Service

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 an manner possible.

Done in 3 ways...

Flawed Implementation

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

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>

Mechanical Turk / “The Turk”

1. SiteA protected by CAPTCHA verification
2. SiteB offers an attractive service (porn, games, etc.)
3. SiteB periodically downloads a CAPTCH from SiteA
4. SiteB presents SiteA’s CAPTCH to a user who must solve it to see the next picture or continue playing
5. SiteB completes the CAPTCA protected process on Site A with the answer supplied by the user

“Windows game which shows a woman in a state of undress when people correctly type in text shown in an accompanying image.”

BBC News

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 talks to 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).”

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 entry. Please call me
0171-3335000***

WebVisum

“WebVisum is a unique browser add on which greatly enhances web accessibility and empowers the blind and visually impaired community by putting the control in your hands! Its aim is to allow you to better enjoy surfing the net and be significantly less dependent upon outside help.”

“Q: How do you solve these wonderful artistic creations known as CAPTCHAs?”

A: It is, at least for now, a trade secret! But you'll find out that our monkeys are really good at it!”

CAPTCHA Solving illegal?

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.

What is the manufacturer/model of the first vehicle you drove?
What is the name of your best friend in high school?
What is your favorite childhood book?
What is your favorite city to visit?
What is your favorite fabric?
What is your favorite garden tool?
What is your favorite holiday?
What is your favorite household tool?
What is your favorite perennial flower?
What is your favorite school subject?
What is your favorite vacation place?
What is your high school's mascot?
What was the name of your first cat?
What was the name of your first dog?
What was the name of your first pet?
Who is your favorite author of all time?
Who is your favorite college professor?
Who is your favorite high school teacher?
Who is your favorite historical figure?
Who was your first employer?

Hi-jack a Sprint user's accounts

With just a
cell phone
number...

Sprint ahead

Shop | My Sprint | Digital Lounge | Support

Answer the following questions

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

Where do these questions come from?

Sprint has partnered with a verification company that has developed an anti-fraud tool that will ask you questions as the account holder. The questions that you will be asked to answer are randomly generated through information regulated by Federal Laws. This anti-fraud tool has been used by numerous industries, including the insurance industry, 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

“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.”

Answer the following questions

Please answer the questions below to verify that you are the account holder and to help us to protect your account 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 verify you as the account holder. The questions that you will be asked to answer are randomly generated through the use of publicly available information regulated by Federal Laws. This anti-fraud tool has been used by numerous industries, as well as the Federal Government after 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 Steff 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: [REDACTED]

* Street Address or PO Box: [REDACTED]

Suite, Apt. or Department: [REDACTED]

* City: WASHING

* State: DC

* ZIP Code: 20012

* Contact phone number: 202 [REDACTED]

* Contact name: [REDACTED]

Email Address: [REDACTED]

Reset

[Add a phone to share minutes](#)

[Change Plan Add-ons](#)

Add-ons for [REDACTED]

<input checked="" type="checkbox"/>	Cellular Call Detail	Included
<input checked="" type="checkbox"/>	Unlimited Nights Weekends-7pm	Included
<input type="checkbox"/>	Picture Mail	\$5.0
<input checked="" type="checkbox"/>	America Expanded Voice Coverag	Included

Check the options you want to add to your

<input checked="" type="checkbox"/>	Mobile Locator™	\$
<input type="checkbox"/>	1000 SMS Text Messages	\$
<input type="checkbox"/>	Sprint Family Locator Service	\$9.99
<input type="checkbox"/>	300 SMS Text Messages	\$5.00
<input type="checkbox"/>	Unlimited SMS Text Messaging	\$15.00

Save changes

[Close](#) ✕

[Payment past](#)

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.

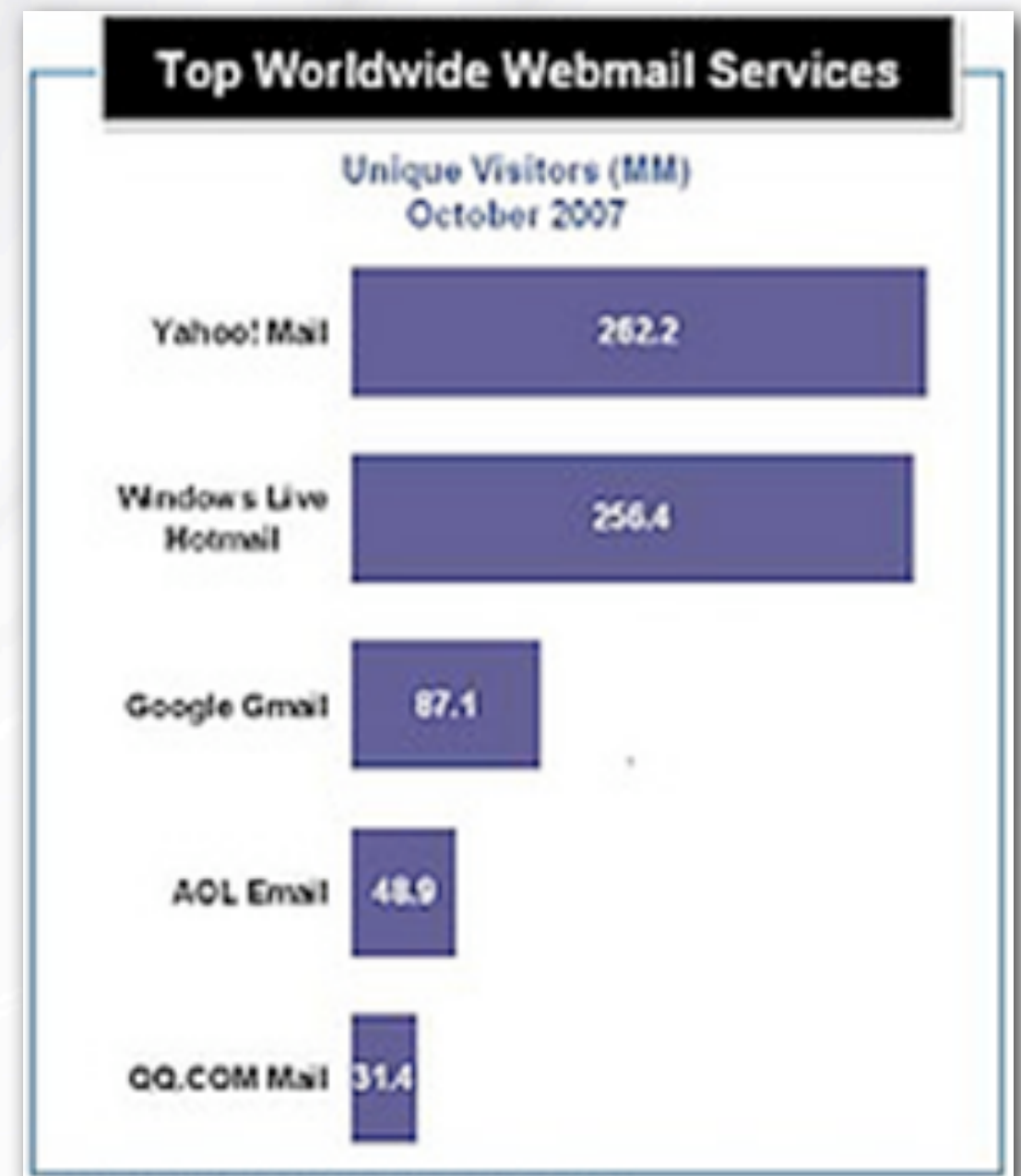
With Web-based Mobile Locator™ you can see the current location of an employee's phone. In real time. In the advanced mapping display on your PC. It's the information you need to provide superior customer service, avoid delays and increase productivity. Or simply enjoy peace of mind.

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



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.

HIRE 2 HACK

LOVE ALL TRUST ME

Block

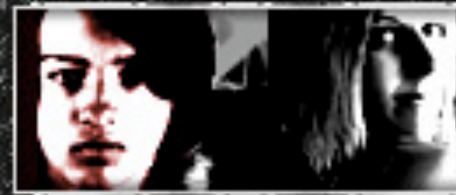


Email Password Recovery

Hire2Hack crack all Yahoo! , MSN, Hotmail, AOL & Gmail passwords in less than 24 hours. Tell us if someone cracks faster, and we give give you a candy !!

Online Infidelity Investigations

Vengeance, is a man's right. Get to the bottom of the truth...is he/she is cheating on you..!! Let us investigate online for you, and uncover the truth for you !!



Internet Spying Services

Victims of Fraud , suspect your partner...or want to keep an eye on your children...? The world is a dangerous place....DO WE NEED SAY MORE ?



Transparent service, safe , secure and quick results.

We are a bunch of freelance hackers...not at all corporate. We are better result-oriented ; and probably are a better value for money, than the other humbugs trying to present HACKING in a legal format. Instead of wasting time faking it, we just CRACK the email address for you ASAP.

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

Your Name	
Your Email Address	
Confirm your Email Address	
Your Country	
<input type="radio"/> Most Urgent <input type="radio"/> Urgent <input type="radio"/> Just do it whenever you can	
Victim Name	
Victim Email Address	
Confirm Victim Email Address	
Victim Country	
Victim Language	
Optional Information :-	
How you know us	
Your Yahoo! Chat ID	
Your MSN Chat ID	
Preferred Mode of Payment	
Bonus offered (if any)	
Any Instructions ?	
<div>Submit your Order</div>	

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

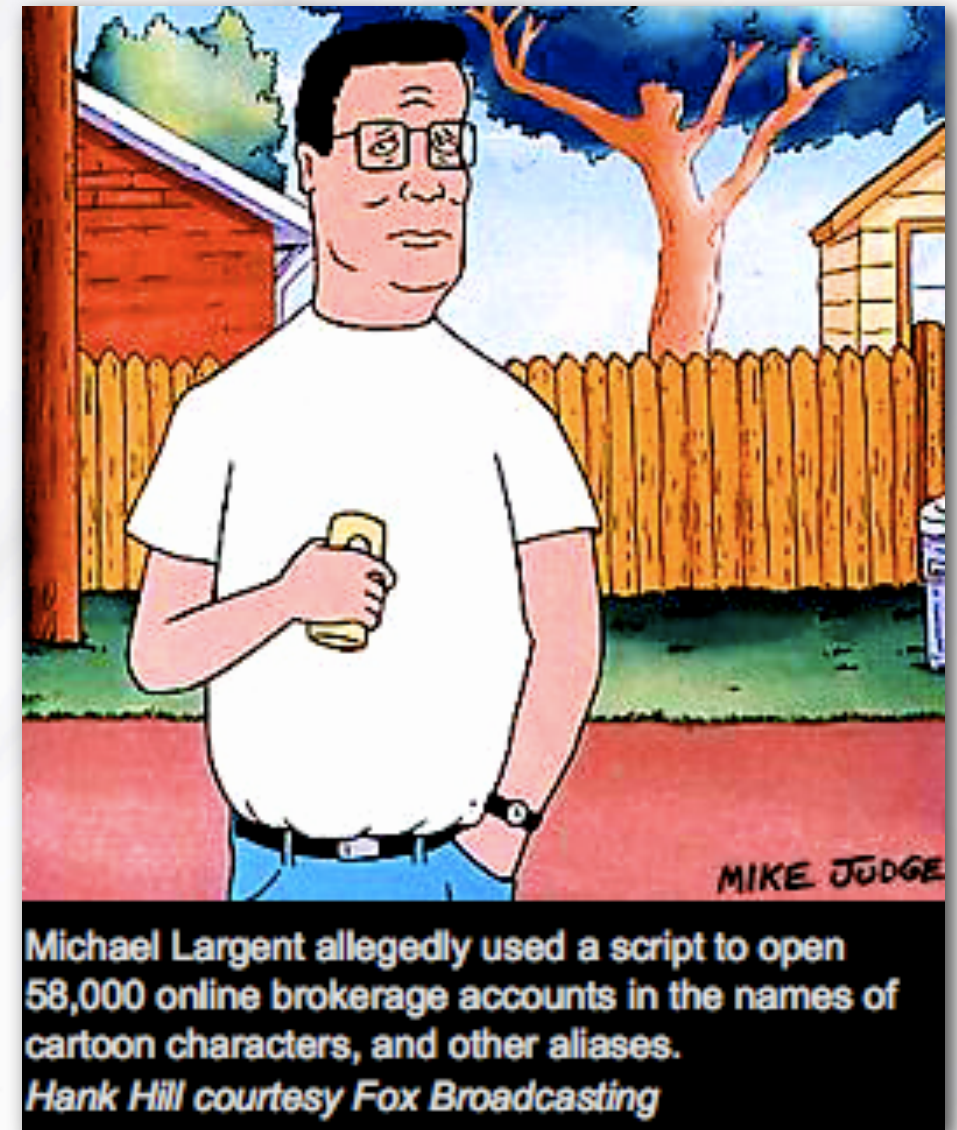
"Micro-deposits" of a random few cents (\$0.01 - \$2.00) are used to verify financial accounts and routing numbers are correct and to verify that customers received it.



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.”

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



Google's Checkout: \$8,225

E-trade, Schwab: \$50,225

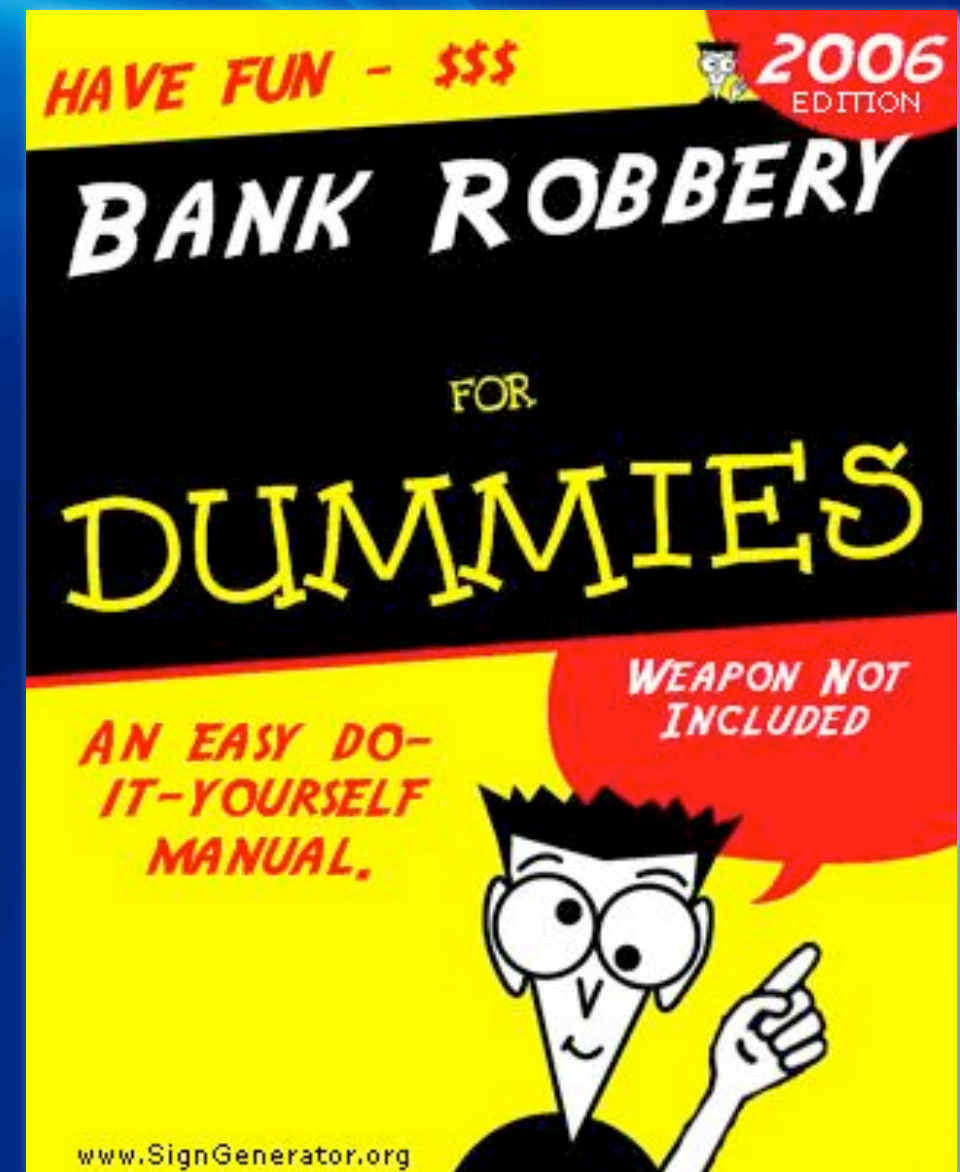
Profited using pre-paid debit cards

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 hacking a single financial institution, an attacker could compromise dozens/hundreds/thousands.



How to hack 600 banks...

- An ASP provides hosting for banks, credit unions, and other financial services companies. ASPs are attractive targets because **instead of focusing 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 a 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

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

- By changing the **acct_id** to an arbitrary yet valid account #, the system would error and say “**Account #X belongs to Bank #Y**”
- If you changed the **bank_id** to #Y, the system would error again and say “**Bank #Y belong to Client #Z**”
- If you changed the **client_id** to #Z, 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

Reverse Money Transfer

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

$$A = A - (\$10,000)$$

$$B = B + (\$10,000)$$

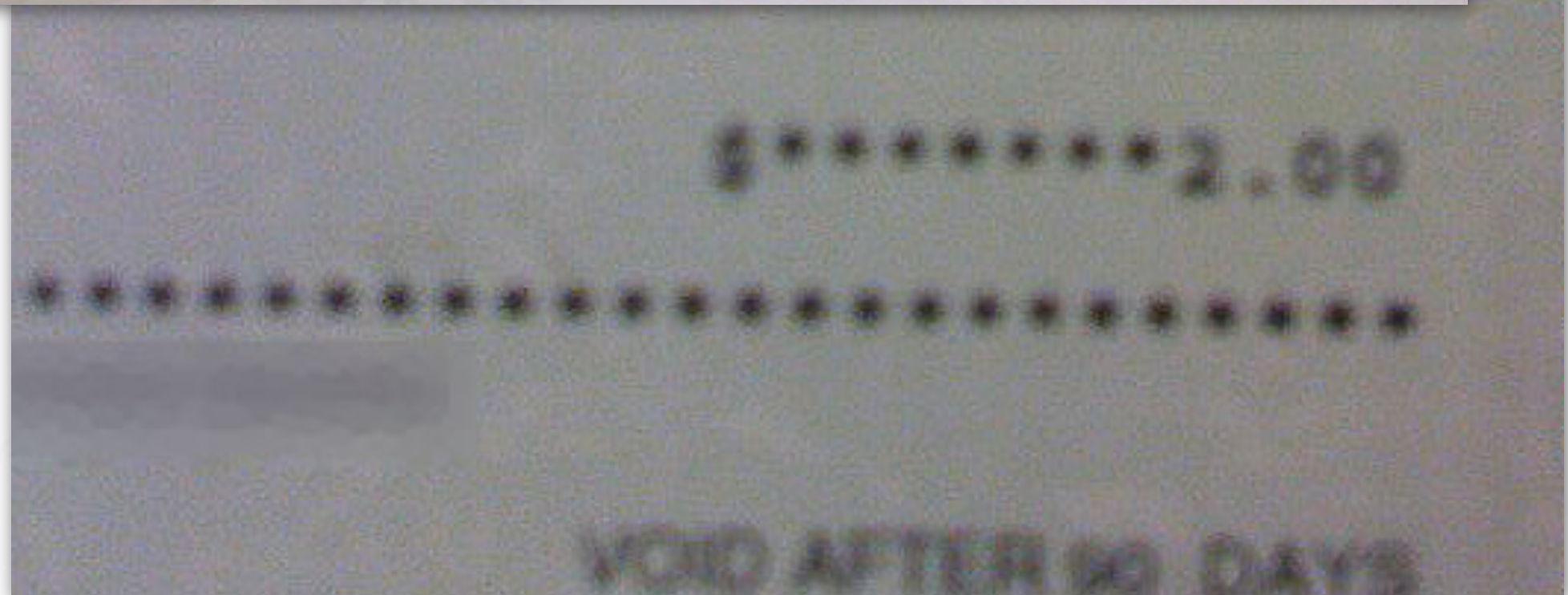
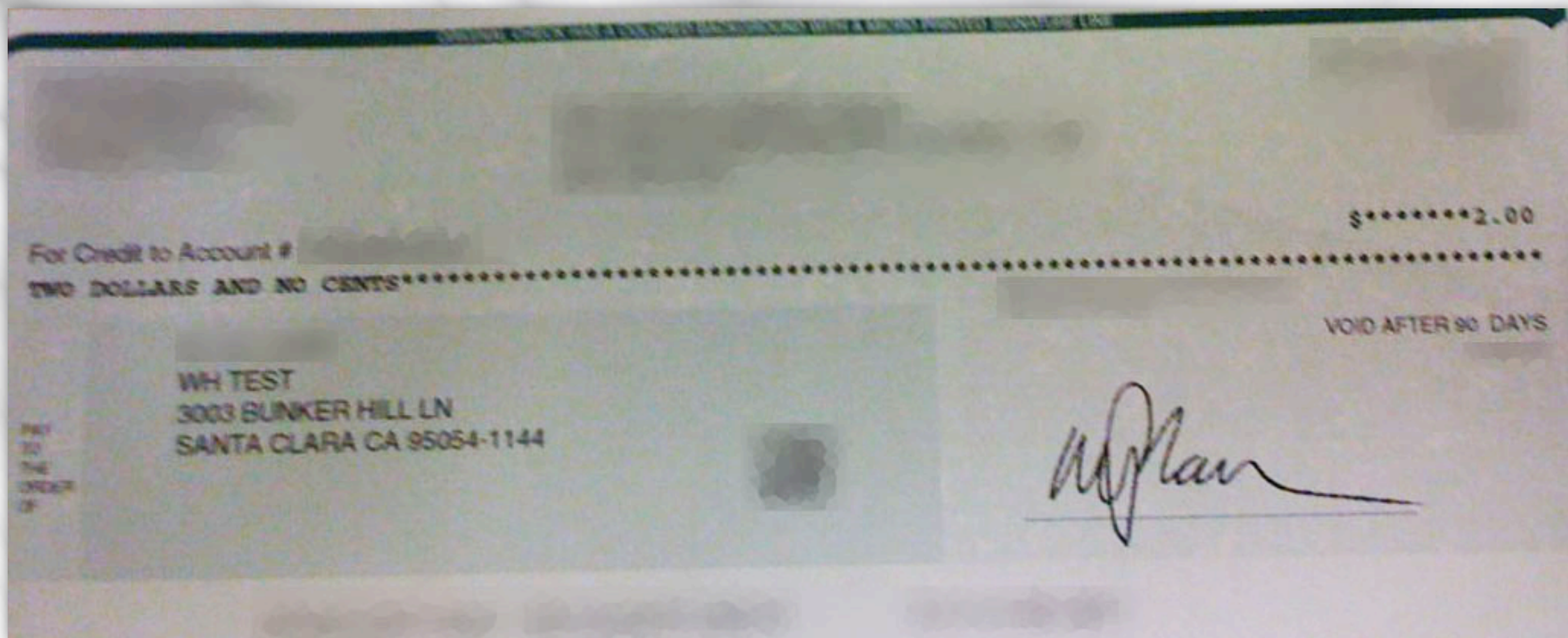
Negative: -\$10,000 from Account A to Account B

$$A = A - (-\$10,000)$$

$$B = B + (-\$10,000)$$

*“Back-end business controls
will prevent these issues.”
ASP Security Contact*

a few week 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 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.

Making Millions by Trading on Semi-public Information



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 its 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.

Business logic flaws = \$\$\$

In 3-5 years XSS, SQLi, and CSRF will be on the way out

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

Thank You!

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

Jeremiah Grossman, founder and CTO

blog: <http://jeremiahgrossman.blogspot.com/>
jeremiah@whitehatsec.com

Arian Evans, Director of Operations

blog: <http://www.anachronic.com/>
arian.evans@whitehatsec.com