

# Everything You Know about Password-Stealing is Wrong

Cormac Herley

Microsoft Research, Redmond

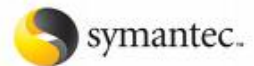
Joint work with D. Florêncio

# What do we know?

## How do we know it?

- **Black Market In Credit Cards Thrives on Web**
  - "Want drive fast cars?" asks an advertisement, in broken English, atop the Web site iaaca.com. "Want live in premium hotels? Want own beautiful girls? It's possible with dumps from Zo0mer."
- **The Underground Economy: priceless**
  - "Even those without great skills can barter their way into large quantities of money they would never earn in the physical world."
- **Symantec Underground Economy Survey**
  - "Symantec has calculated that the potential worth of all credit cards advertised during the reporting period was US\$5.3 billion."
- **A Field Day for Financial Cyber-Scammers**
  - "Total losses from cyber-related crime at financial institutions topped \$20 billion last year, estimates security consultant Lance James"
- **Phishing losses up to \$3.2bn**
  - "An online survey has pegged the soaring losses from phishing attacks this year at \$3.2 billion, according to new research from Gartner."

The New York Times



**BusinessWeek**

**Gartner.**

Navigation / Search

Share

Help



1

“

THE SHOCKING SCALE OF  
CYBERCRIME

PLAY AGAIN

\$388  
BILLIONTHE TOTAL BILL FOR CYBERCRIME FOOTED BY ONLINE  
ADULTS IN 24 COUNTRIES TOPPED USD \$388BN OVER  
THE PAST YEARVICTIMS VALUED  
THE TIME THEY  
LOST TO CYBER-  
CRIME AT OVER

\$114bn

\$274bn

THE DIRECT CASH COSTS OF  
CYBERCRIME - MONEY STOLEN  
BY CYBERTHUGS/SPENT ON  
RESOLVING CYBERATTACKS -  
TOTALLED \$114BN

“

CYBERCRIME IS BIGGER  
THAN......the global black market in **marijuana, cocaine and heroin** combined (\$288bn) and approaching the value of all **global drug trafficking** (\$411bn) iAt \$388bn, cybercrime is more than **100 times** the **annual expenditure of UNICEF** (\$3.65 billion) ii

431

1m+

14

SUMMARY: THE SHOCKING SCALE OF CYBERCRIME

# Outline

- Consumers are not liable for losses
- Emptying accounts is hard
- Passwords are not the bottle-neck
- Underground markets are not thriving
- Credential stealing is a terrible business

# Consumers are not liable for losses

FBI Director Robert Mueller was banned by his wife from doing online banking after he nearly fell for a phishing scam. “No more Internet banking for you” she said.



# Regulation E

- US Federal Reserve *Regulation E* limits user liability to \$50
  - “any electronic transfer that is initiated through an electronic terminal, telephone, computer or magnetic tape.”
  - “*Consumer negligence*. Negligence by the consumer cannot be used as the basis for imposing greater liability than is permissible under Regulation E. Thus, consumer behavior that may constitute negligence under state law, such as writing the PIN on a debit card or on a piece of paper kept with the card, does not affect the consumer's liability for unauthorized transfers.”



“Bank of America's Zero Liability Guarantee, for example, guarantees zero liability for any unauthorized activity originating from Online Banking or Bill Pay.”

Source: [www.bankofamerica.com](http://www.bankofamerica.com)



“We guarantee that you will be covered for 100% of funds removed from your Wells Fargo accounts in the unlikely event that someone you haven't authorized removes those funds through our Online Services.”

Source: [www.wellsfargo.com](http://www.wellsfargo.com)





“We will reimburse your Fidelity account for any losses due to unauthorized activity.”

Source: [www.fidelity.com](http://www.fidelity.com)



“Under HSBC's \$0 Liability, Online Guarantee, you are covered 100% and liable for \$0.”

Source: [www.us.hsbc.com](http://www.us.hsbc.com)



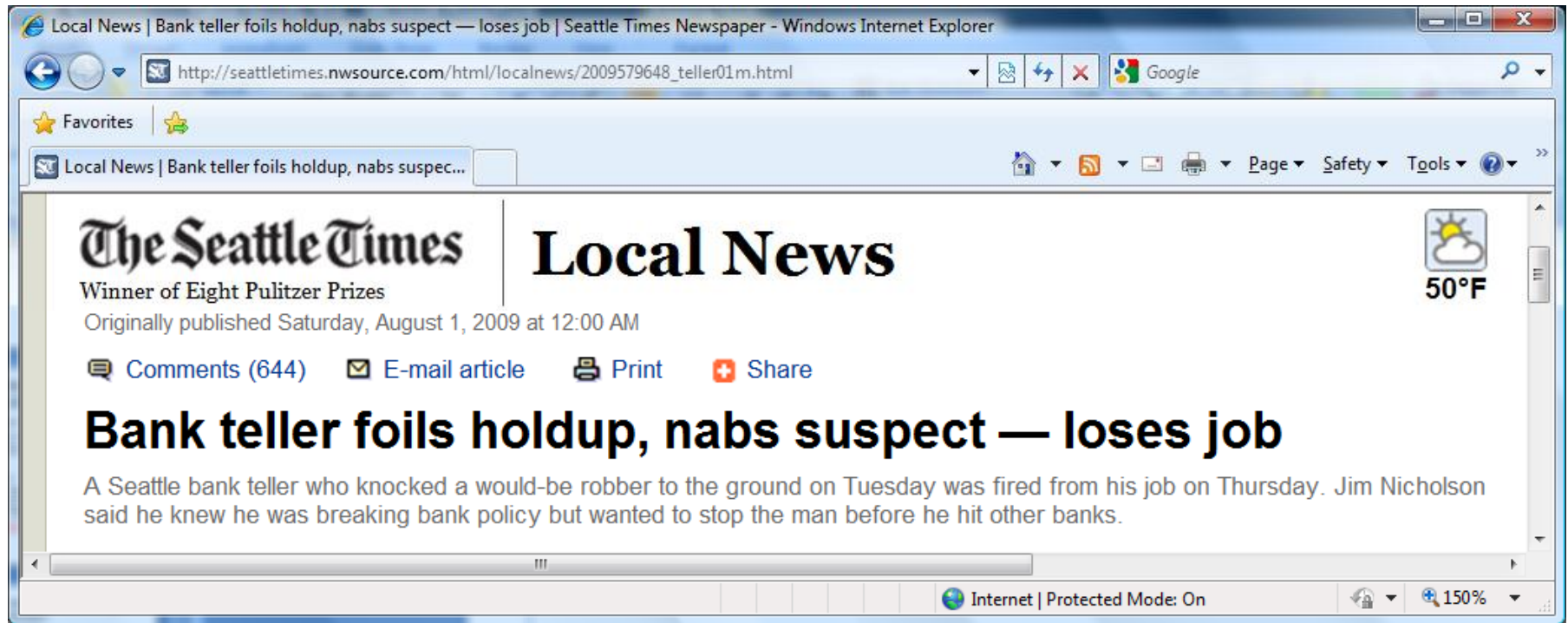
“PayPal currently voluntarily reimburses consumers for all financial losses from transactions not authorized by the consumer, not just losses above \$50.”

Source: Dec. 2009 10-K filing

# Other jurisdictions etc

- EU Directive 61: 150 euros
- Canadian banks: zero liability

Idea that consumers suffer irreversible financial harm is incorrect.



**Banks understand:**

- 1. Fear is bad for business**
- 2. Getting money not the same as keeping it**
- 3. Non-repudiation**

**Emptying Accounts is Hard**

# Thief gets nothing if transfer is:

Detected



Reversed



Traced



# Untraceable Irreversible transactions are hard to repudiate

- Suppose not: banks have no protection against first part fraud (self-theft).
  - E.g. Alice wires life savings to another acct
  - Claims “I’ve been robbed!!!”
  - Demand refund under Regulation E, Zero Liability
- This only works if transaction can’t be
  - Traced or reversed.

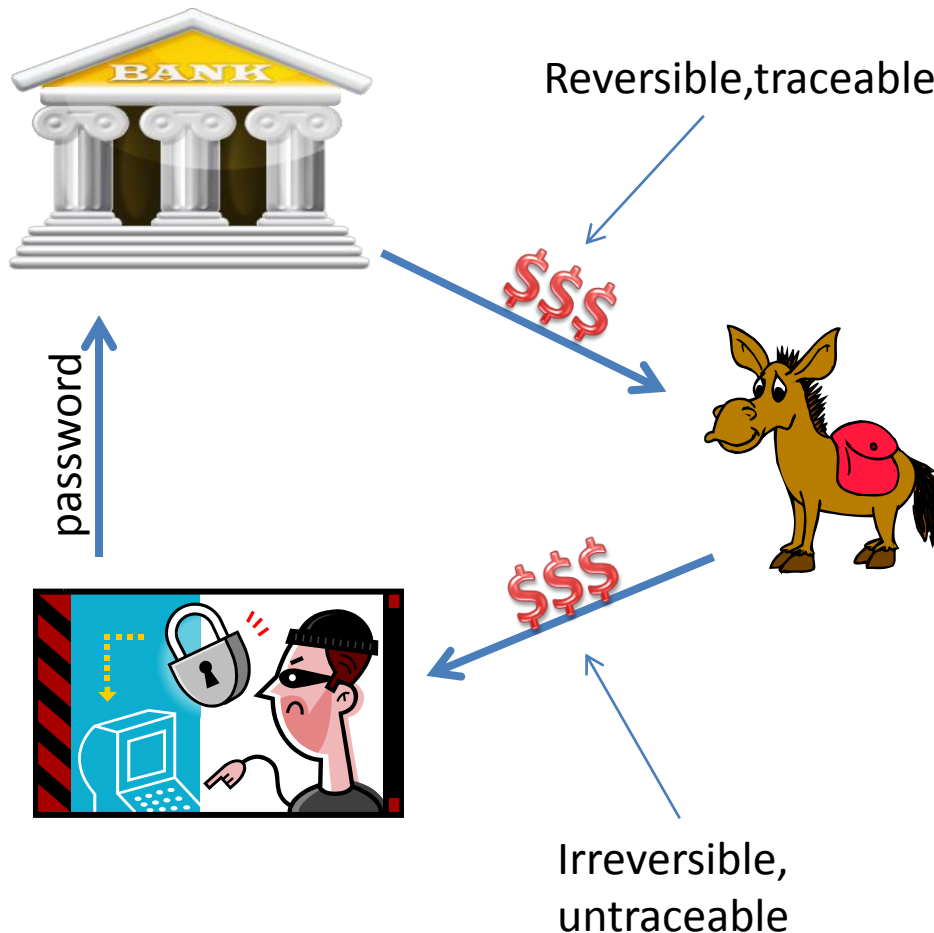


# So transaction must be

- Irreversible
- Untraceable
- But this is hard in the banking system
  - Bank Secrecy Act (1970)
  - US Patriot Act (2001)

*“All problems in computer science can be solved by another level of indirection”*  
*B. Lampson*

# Mule: turn reversible/traceable transaction into irreversible/untraceable



- Wire money to mule
- Mule uses
  - WesternUnion
  - VirtualGold
  - eCash etc
- Trace only to mule
- Reverse only from mule

# Mule (aka work-at-home schemes)

- Mule is given semi-plausible reason to “process transactions”
- Receive funds from victim acct
  - Reversible
  - Traceable
- Send funds to attacker
  - Irreversible
  - Nontraceable
- Mule gets 10-20% “commission”
- Mule never meets “employer”
  - Uses only cash, unstoppable transfers
  - Urgency is a common theme

LYDON ONLINE  
Private Business Solutions

Hi Log out

HOME AGENTS AWARDS SOLUTIONS CONTACT US search...

Best Performance Agent Preparation

**DIVISION MANAGER**  
Lance S. Turner

**TEAM LEADER OF THE QUARTER**  
Shelly D. Daniels

**AGENT OF THE QUARTER**  
Jessica L. Howard

Online Support Notifier

Private Messages no new

Support Mailbox

Agent Prep

Modification

YouTube

Agent Preparation consists of a video that will assist you with your upcoming order. Above you will see the Agent Preparation video. Be sure to "Pause" the video when necessary and listen to it as many times as you need to. If you are not able to view the above video in your browser, please notify Management via the Check-In form on the website.

**Agent Appreciation**

We take great pride in acknowledging and honoring our agents with the recognition they deserve. This process motivates junior agents to excel in the same manner.

**Staff Notice**

All hands staff meeting will take place twice daily. Current meeting times are start of business and close of business each day. Staff should ensure at least one of their team members are present at both meetings.

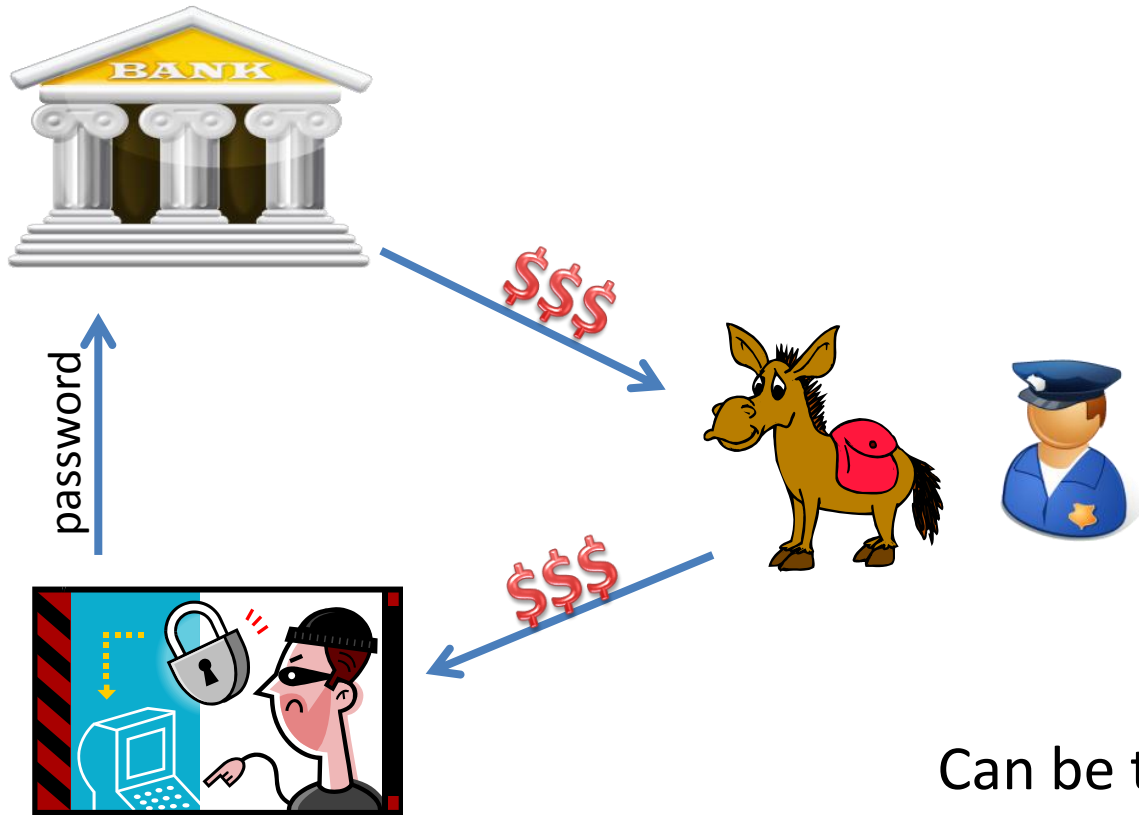
**Agent Notice**

All Senior Agents interested in the upcoming TeamLeader position should be sure to get with their Division Manager to submit the TLA.

Q: Why doesn't attacker just use, e.g., Western Union directly?

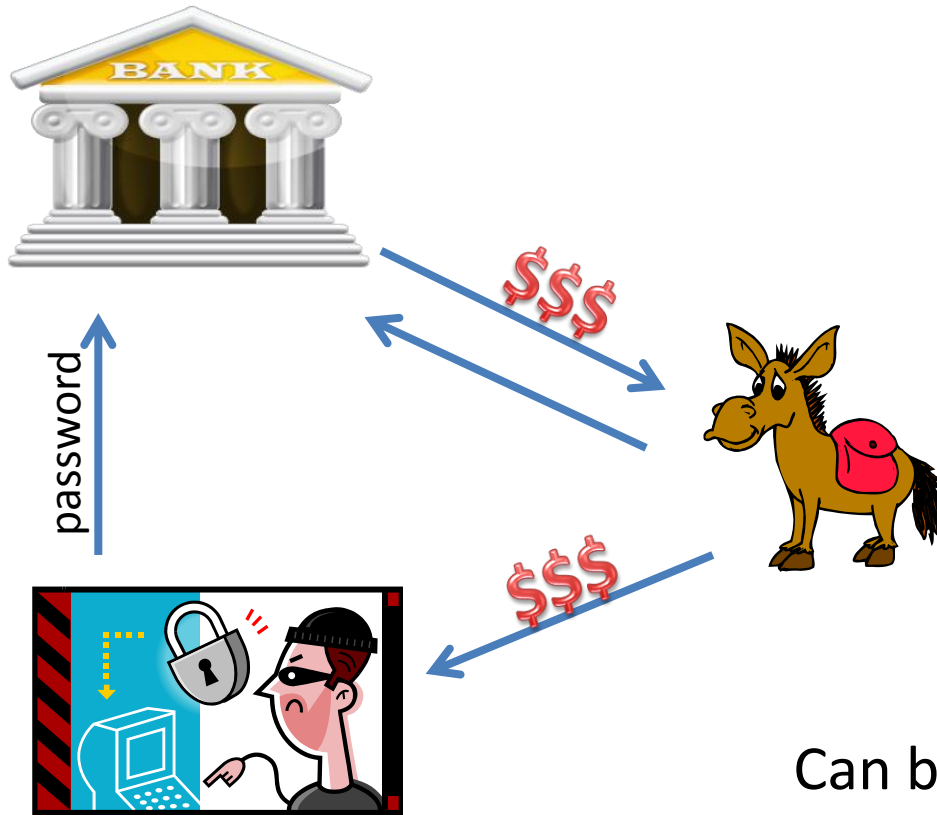
A: Requires ID or signature on victim acct

# When Transaction is traced



Can be traced only to mule

# When Transaction is reversed



Can be reversed only from mule

# Start to finish

Phisher steals \$10k from victim acct

	Before discovery	After discovery
Victim	-\$10000	\$0
Bank	\$0	\$0
Mule	+\$1000	-\$9000
Attacker	+\$9000	+\$9000

**Attacker stole  
From mule not victim!**

- Attacker stole from mule, not from victim or bank!!
- Mule has no consumer protection
  - (Reg E doesn't apply: initiated the transfer)

# Banks understand non-repudiation

**Claim\*:** if can be repudiated it can be reversed

**Sketch of Proof:** Multiply any repudiable non-reversible transaction by 100m/day.

	Reversible	Non-reversible
Repudiable	My CC payment Checks ETF	?
Non-repudiable		Cash at ATM Western Union Moneygram

\* US consumer accts only, Your mileage may vary.

Passwords are not the bottle-neck



- “Most money mules get a single transfer”  
Krebs (May 11, 2010)
- “Ratio of stolen credentials to mule capacity could be as high as 10000 to 1” Cisco Annual Security Report
- Recruiting/running mules is high-touch

# Passwords are not the bottleneck

- Stealing passwords is easy
- Cashing out is hard
- Oversupply of credentials on underground economy
- Harm done  $\propto$  outflow, not inflow



# Underground Markets are not Thriving

“In the Underground Economy even those without great skills can barter their way into large quantities of money they would never earn in the physical world.”

[Thomas and Martin, ;login 2006]

# Why do Credentials sell for pennies on dollar?

- Symantec: “CCN’s sell for \$0.5 to \$12”
- Cymru: \$500 for face value \$10million creds
- Franklin etal.: 465 free CCNs/day on single channel
- Offered Explanations:
  - More supply drives price down [Symantec]:
    - But demand for free money is infinite?
  - Volume Sellers don’t care [Cymru]:
- **Nobody sells gold for the price of silver**

# Offers to Buy, Offers to Sell

- Published accounts on underground economy:
  - No observed transactions
  - \$0 changing hands
- Offers to sell greatly outnumber offers to buy
- Participantion:
  - Anonymous
  - Scriptable
  - Cheating is ubiquitous
- Sort of like netnews w/o the quality control

# How Can Market Function when Cheating is Common?

- Thomas & Martin [login 2006]
  - “Each IRC network will normally have a channel, such as #help or #rippers, dedicated to the reporting of those who are known to conduct fraudulent deals.”
- Symantec: [Underground Econ Report]
  - Many IRC servers have channels listing current rippers
- Franklin et al [CCS 2007]
  - 22% of posted CCNs failed Luhn checksum
  - Utilities provided by channel admin designed to steal CCNs
- Dhanjani and Rios [Blackhat 2008]:
  - Backdoors common in for-sale phishing kits/tutorials
- Cova et al [WOOT 2008]
  - Obfuscated backdoored phishing kits
- Countermeasures ought to be easy.  
(Franklin et al [CCS 2007])

```
NO MORE BOTS . JUST PLZ USERS : )
```

```
12:31 > [redacted] I am a legit drop for ITems In US , you can trust me 100 % , i also can cashout  
on any id n name just try me !  
12:31 > [redacted] Scot poste it , [redacted], cauti persoane care incarca cartile de it . Lasă un id dacă  
nu sunt !  
12:31 > [redacted] / Selling Cvv2 & Full info (US) - (FR) | Selling Mailist Virgin From Shop  
Admin (UK) - (US) - (FR) | Selling Host Hacked | Webmail | Upload All Scam  
Page | Upload PHP Nailer | Selling Fast VPN | Selling RDP & VPS & VNC |  
Selling Account Socks All Word ~ I Accept Only [redacted]  
12:31 > Spamm All Banks UK / US * I Can Ship To All Address ( Europ - USA ) *  
Spamm Private For Any Client * I Accept Only [redacted] Or  
12:31 < [redacted] /\ Selling Dumps Track 1 & 2 With Pin /\ Selling Shop Admin US With Big  
& Small Daily Order /\ Selling Serial Camfrog & Palstalk /\ Selling  
Software Find Fresh Mailist Perfect /\ Selling Shell C99 /\ Selling Root  
\ \ ~ I ACCEPT ONLY [redacted].  
12:31 ? Chkon mscr206 msq gdw  
12:32 selling account SMTP inbox (send to your index for test)...also selling US  
& UK mailist...selling host Support Cpanel+ftp...selling smtp scanner &  
SSH Scanner POP3 Scanner SQL scanner & CVW ALL COUNTRY for serious buyer  
payment only KIFFER [redacted]  
12:32 > Set your timers on [redacted], usins >> "/timer 0 50/msd [redacted] your message here  
" Enjoy your stay!!  
12:32 ? Selling Fresh Dumps, Cv2 & Fulls, USA / CAN / UK / Europe. Spammed &  
Hacked Shop Admin. Accepting + +.  
12:32 ? I Can CASBOUT UK Cvw With DOB,[redacted]  
12:32 selling account SMTP inbox (send to your index for test)...also selling US  
& UK mailist...selling host Support Cpanel+ftp...selling smtp scanner &  
SSH Scanner POP3 Scanner SQL scanner & CVW ALL COUNTRY for serious buyer  
payment only KIFFER [redacted]  
12:32 ? free socks http://[redacted]/ user:[redacted] pas : [redacted]  
12:32 > Selling Hacked Cpanel, Selling Fresh Mall leads for USA / UK / Nero (MAIL  
List). Selling Acces [redacted] login with verified, Selling [redacted] login with email  
access, Selling IP Stock Any Country ---- Payment mode [redacted] &  
www.[redacted]  
12:32 > Selling logins with fulls info-selling good fpp / vnc /account socks/fulls  
pc and good valid cvw -sell fresh shop admin -sell fresh mailist intouchad  
from shop admin-upload all scam - Payment mode, [redacted] and only  
12:32 ? Chkon mscr206 msq gdw  
12:32 ? SELLING WU BUG 800 BITS ALL AVAILABLE BINLS , Transfer to USA 100% SUCCESS,  
Transfer to other country SOL SUCCESS. Payment in dynamis or
```

# Symantec:

“Potential value of CCNs stolen \$5.3bn”

- Sum of asking prices: \$163 million
- [Total offered for sale] x  
FTC Avg CCN fraud \$5.3 billion
- So Symantec estimate = [Sum of asking prices] x 32
- **This assumes:**
  - 100% of goods offered on IRC channels sell (at asking price)
  - Banks detect 0% of attempted fraud
  - Rippers account for 0% of sales
  - Sellers give buyers 30x return

# A Simpler Explanation

- Buyers demand 5x return
- Final price 50% of ask
- Assume 10% of offered creds sell *and* are good
- Total CC fraud from channels:  
$$163 \times 5 \times .5 \div 10 = \$41 \text{ million}$$
- **Factor difference with Symantec: 128x**
  - Extrapolating from \$0 to \$5.3 bn is a big jump



# Credential Stealing as a Business

“We try to buy businesses with intrinsic durable competitive advantages.” Charlie Munger

- No barrier to entry
- No protection for
  - Intellectual property
  - Brand loyalty
  - Customer lockin
- No contract enforcement

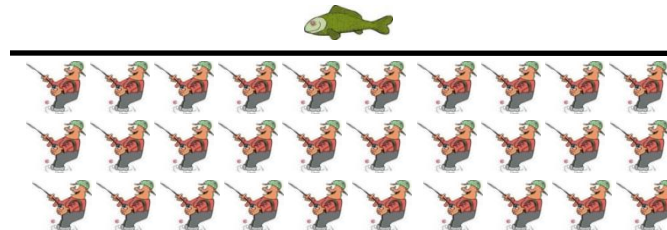
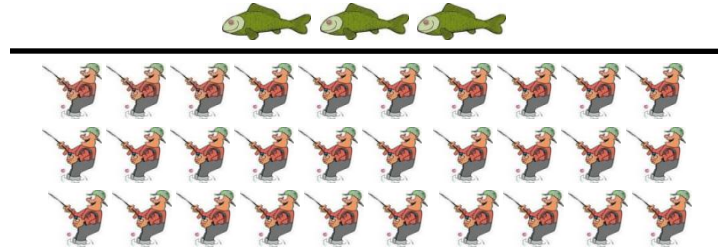
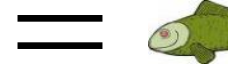
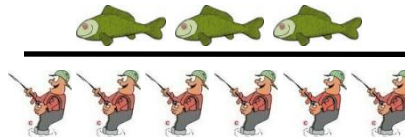
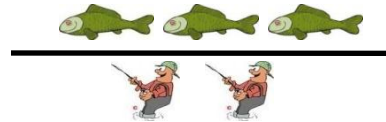
# Open Access Resources

- ***Open access to the resource***, i.e. no barrier
  - Anyone who wants to fish/phish can exploit
- Tragedy of the Commons
  - Fishing ground yields far less than it is capable of
  - Phishing yields far fewer dollars than possible

# A Quick lesson in Competition

$$\text{Return} = \frac{\text{Victims}}{\text{Phishers}}$$

↓  
More  
Phishers



Less Phish?

# The squeeze on phishing

- Return = Victims/Phishers
- Denominator increasing (“free money!!!!”)
- Numerator decreasing. Why?
  - ***Because*** the denominator is increasing
  - Technical measures: browser warnings etc
  - Fraud detection: banks get better
  - Users learn: nobody gets phished 10 times.

“If it sounds too good to be true  
then it is.”

NIST advice on cyber-scams

Sound advice when counseling users on mule recruitment,  
Nigerian scams etc. How come we forget it when considering  
the prospects for scammers?

**“But, they wouldn’t be doing this if  
they weren’t making money”**

# Effort $\neq$ Dollars

Attempt to reach: 100000  
Reach Klondike: 20000  
Pan for gold: 12000  
Find any gold: 4000  
Get rich ( $> \$5k$ ): 300

Gold extracted: \$50 million  
Goods sold: \$100 million



Prospectors on the way to the Klondike 1897



# “They wouldn’t be doing it if they weren’t making money”

- No. They think they’re going to make money
- Where would they get that idea?

- ◉ Black Market In Credit Cards Thrives on Web

The New York Times

- “Want drive fast cars?” asks an advertisement, in broken English, atop the Web site iaaca.com.  
“Want live in premium hotels? Want own beautiful girls? It’s possible with dumps from Zo0mer.”

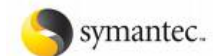
- ◉ The Underground Economy: priceless

- “Even those without great skills can barter their way into large quantities of money they would never earn in the physical world.”



- ◉ Symantec Underground Economy Survey

- “Symantec has calculated that the potential worth of all credit cards advertised during the reporting period was US\$5.3 billion.”



- ◉ A Field Day for Financial Cyber-Scammers

- “Total losses from cyber-related crime at financial institutions topped \$20 billion last year, estimates security consultant Lance James”

BusinessWeek

**When we encourage overestimation of returns we make things worse.**

# **Sex, Lies and Cyber-crime Surveys**

Navigation / Search

Share

Help



1

“

THE SHOCKING SCALE OF  
CYBERCRIME

PLAY AGAIN

\$388  
BILLIONTHE TOTAL BILL FOR CYBERCRIME FOOTED BY ONLINE  
ADULTS IN 24 COUNTRIES TOPPED USD \$388BN OVER  
THE PAST YEARVICTIMS VALUED  
THE TIME THEY  
LOST TO CYBER-  
CRIME AT OVER

\$114bn

\$274bn

THE DIRECT CASH COSTS OF  
CYBERCRIME - MONEY STOLEN  
BY CYBERTHUGS/SPENT ON  
RESOLVING CYBERATTACKS -  
TOTALLED \$114BN

“

CYBERCRIME IS BIGGER  
THAN......the global black market in **marijuana, cocaine and heroin** combined (\$288bn) and approaching the value of all **global drug trafficking** (\$411bn) iAt \$388bn, cybercrime is more than **100 times** the **annual expenditure of UNICEF** (\$3.65 billion) ii

431

1m+

14

SUMMARY: THE SHOCKING SCALE OF CYBERCRIME

Cyber-crime: “the largest transfer of wealth in history.” K. Alexander, Dir. NSA



- Cybercrime estimates come from surveys

$$Estimate = \frac{|X|}{|R|} \sum_{i \in R} f[r_i]$$

- Surveys are reliable, right?

# “You should never trust user input”

Writing Secure Code, Howard et al.

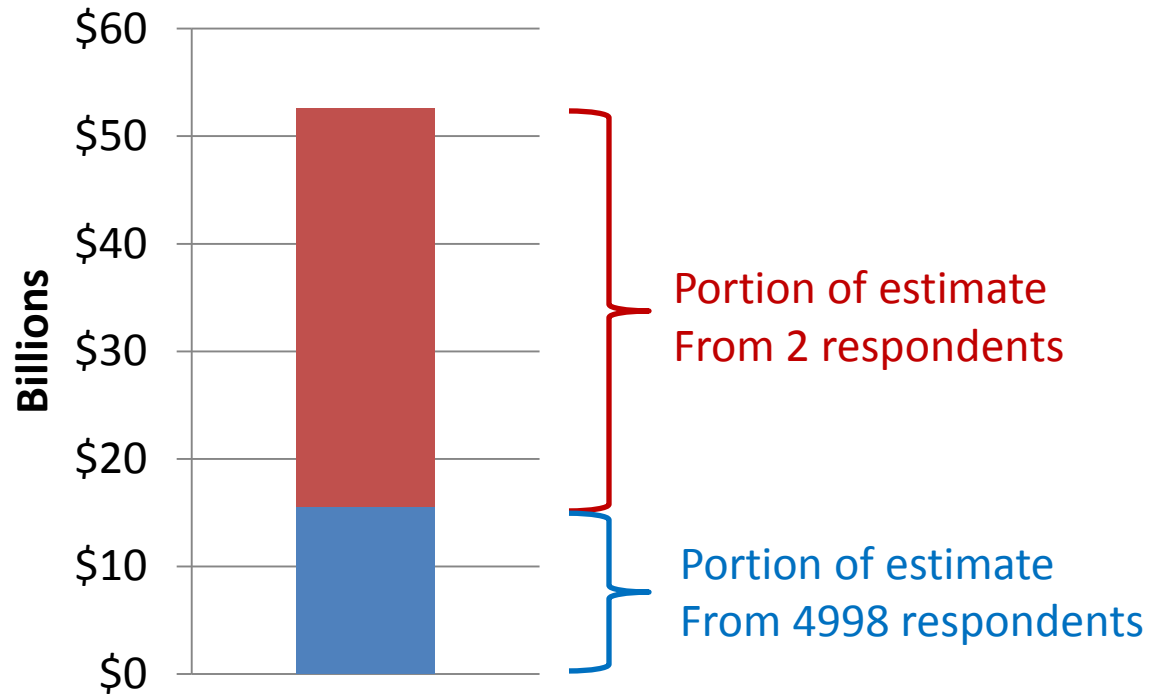
- Importance of input validation in security
  - SQL Injection
  - Buffer overflows

$$\frac{|X|}{|R|} \sum_{i \in R} f[r_i] \quad \equiv$$

```
total = 0.0;
for (i=0; i < survey_size; i++){
    total += (double) strcpy(user_input[i]);
}
estimate = total * population_size/survey_size
```

- Practice unacceptable in writing code ubiquitous in forming estimates

## FTC '06 ID Theft Survey



- Two respondents contribute a factor of  $\frac{37}{2} / \frac{15.6}{4998} = 5927$  more than average
- Two vote at 6000x strength of everyone else.

# Conclusions

- Banks understand non-repudiation
- Passwords are not the bottle-neck
- If it sounds too good to be true then it is
  - Cyber-crime is not easy money
- Never trust user input
  - Most cyber-crime estimates you've seen are junk



# Supporting Documents

- D. Florêncio and C. Herley, ["Is Everything We Know about Password-Stealing Wrong?"](#), IEEE Security&Privacy magazine, to appear
- D. Florêncio and C. Herley, ["Sex, Lies and Cyber-crime Surveys"](#), WEIS 2011