

Cybercrime & the Internet user:

If things are so bad how come they're
so good?

Cormac Herley

Microsoft Research, Redmond

[@cormacherley](#)

1 “ THE SHOCKING SCALE OF CYBERCRIME

PLAY AGAIN ▶

“ CYBERCRIME IS BIGGER THAN...



\$388 BILLION



...the global black market in **marijuana, cocaine and heroin** combined (\$288bn) and approaching the value of all **global drug trafficking** (\$411bn) i

431

At \$388bn, cybercrime is more than **100 times** the **annual expenditure of UNICEF** (\$3.65 billion) ii

1m+

SUMMARY: THE SHOCKING SCALE OF CYBERCRIME

THE TOTAL BILL FOR **CYBERCRIME** FOOTED BY ONLINE ADULTS IN **24 COUNTRIES** TOPPED USD \$388BN OVER THE PAST YEAR +



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



14

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



❖ 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 New York Times

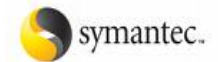
❖ The Underground Economy: priceless

- ❖ "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

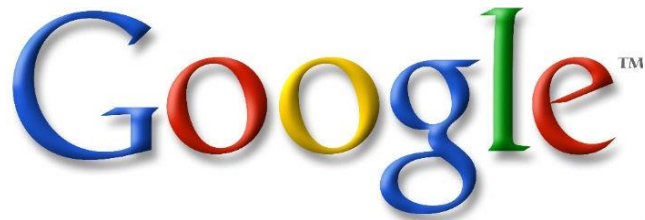
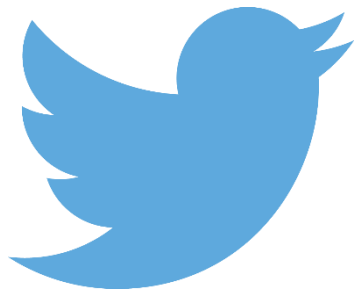
- ❖ "Total losses from cyber-related crime at financial institutions topped \$20 billion last year, estimates security consultant Lance James"

BusinessWeek

- ❖ "Phishing is believed to be growing at a CAGR of 1600% per year"

Scale, anonymity, action-at-a-distance

But they're also pretty good



The image shows a browser window displaying a Wired article. The browser's address bar shows the URL 'http://www.wired.com' and the page title 'Kill the Password: A String of Characters Won't Pro...'. The Wired logo is visible in the top left, and a 'SUBSCRIBE' button is in the top right. The article's main heading is 'HOW TO SURVIVE THE PASSWORD APOCALYPSE'. Below the heading is a sub-headline: 'Until we figure out a better system for protecting our stuff online, here are four mistakes you should never make—and four moves that will make your accounts harder (but not impossible) to crack.—M.H.' To the left of the main content is a 'SHARE' sidebar with social media icons for Facebook (8045 shares), Twitter (630 shares), Pinterest, a comment icon (2 comments), and an email icon. The main content area features a large red 'DON'T' heading followed by a list of four password-related mistakes, each with a right-pointing arrow icon.

HOW TO SURVIVE THE PASSWORD APOCALYPSE

Until we figure out a better system for protecting our stuff online, here are four mistakes you should never make—and four moves that will make your accounts harder (but not impossible) to crack.—M.H.

DON'T

- ▶ **Reuse passwords.** If you do, a hacker who gets just one of your accounts will own them all.
- ▶ **Use a dictionary word as your password.** If you must, then string several together into a pass phrase.
- ▶ **Use standard number substitutions.** Think "P455w0rd" is a good password? N0p3! Cracking tools now have those built in.
- ▶ **Use a short password**—no matter how weird. Today's processing speeds mean that even passwords like "h6lr\$q" are quickly crackable. Your best defense is the longest possible password.

We all ignore most of this, and things still muddle along.

1. Where do security policies come from?



Maynooth University - My Password



Manage Your Password

Password Guidelines

It is very important that you never share your Maynooth University password with anyone.

You should choose a password that is both memorable, and secure. The shorter your password is, the more important it is to include mixed case, digits, and symbols.

We recommend the following:

- Passwords less than 12 characters long should contain mixed case letters, digits, and symbols.
- Passwords between 12 and 15 characters long (inclusive) should contain mixed case letters and digits.
- Passwords between 16 and 19 characters long (inclusive) should contain mixed case letters.
- Passwords 20 characters or longer can contain just a single case of characters.

Register For Password Reset

If you register for Self Service Password Reset (SSPR), you will be able to re-set your password yourself should you ever forget it. *If you do not register, you will have to call in to IT Services reception with your university ID card during office hours to get your password reset.*

[Register for SSPR](#)

Reset Password

If you have registered for Self Service Password Rest (SSPR), click the button below to reset your password.

[Reset Password](#)

If you need your password reset, but have

Change Password


If you would like to change your password, and know your current pasword, please use this form.

Username:

Current Password:

New Password:

New Password (Repeat):

I'm not a robot  reCAPTCHA
Privacy - Terms

[Change Password](#)



WA 520 Toll Bridge

Washington State Department of Transportation | goodtogo 520

Page | Safety | Tools

First Name * MI Last Name *

Company Name

E-mail Address *

Verify E-mail *

User ID * Do not use spaces or special characters.

Password * At least 8 letters/numbers (at least one upper case, one lower case and one number). No spaces or special characters.

Verify Password

Security Question * What is your mother's maiden name?

Security Answer * At least 2 letters/numbers. No spaces or special characters.

Verify Security Answer *

Security Question * What was the name of your first (elementary) school?

Security Answer * At least 2 letters/numbers. No spaces or special characters.

Verify Security Answer *

Security Question * What is your brother's middle name?

Security Answer * At least 2 letters/numbers. No spaces or special characters.

Verify Security Answer *

4 Digit PIN * Allows you to manage your account with the automated phone system.

Promotion No promo code needed to get \$10 in free tolls.

Internet | Protected Mode: On | 150%

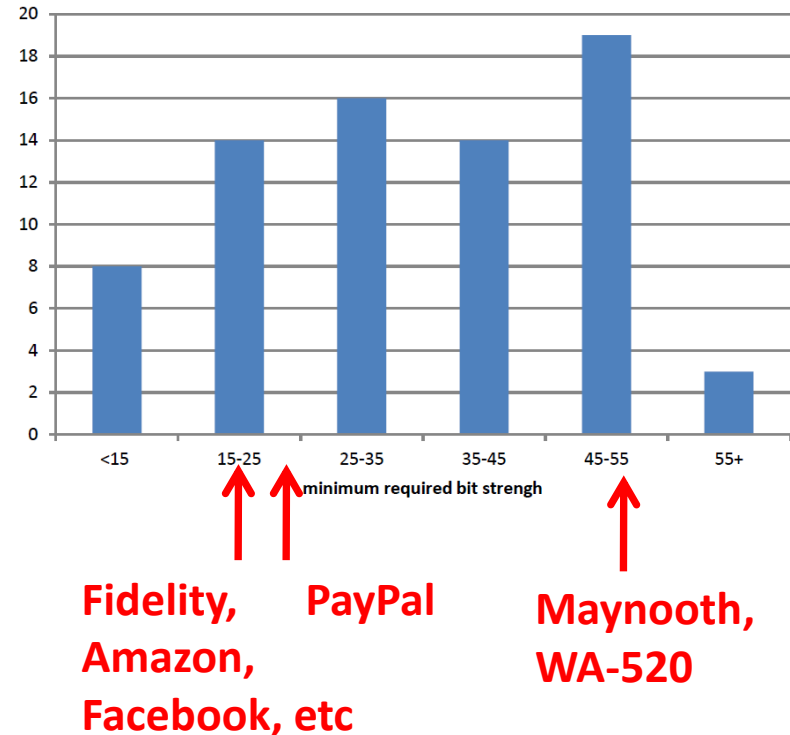
How Does this Compare to Everyone Else?

- Password polices 75 sites
 - Top 20 traffic, 10 medium
 - Top 10 financial, .gov, .edu

Fidelity: \$2 trillion assets

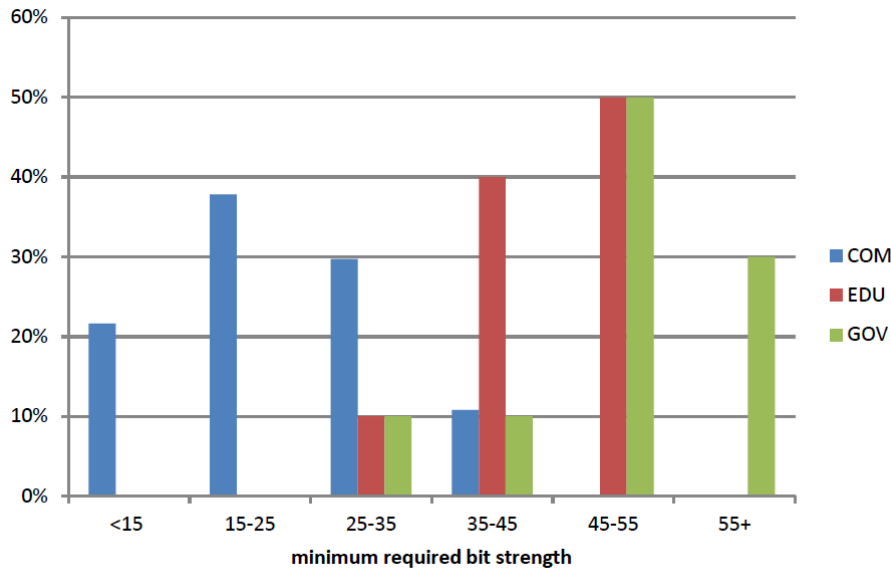
Amazon: largest online retailer

Paypal: most phished site on the web



If Amazon can manage with 6 chars why can't everyone?

Split histogram by .com, .edu, .gov



Sites	Median Strength
Top Traffic	19.9
Medium Traffic	19.9
Financial	31.0
Large Universities	44.5
Government	47.6
Accept adverts	19.9
No adverts	44.3

Every login event is a revenue opportunity for Amazon, Fidelity, Paypal, facebook.
Every login event is cost for Maynooth, and WA-520.

Moral: money and incentives reveal a lot about where things reach equilibrium

Security, Usability and Equilibrium

- WA-520.wa.gov is simply better insulated from consequences of poor usability.
- Every time you login at Amazon you are revenue; every time you login at Maynooth you are cost.



WA-520.wa.gov



Amazon.com



2. Why do Nigerian Scammers say they're from Nigeria?

I NEED YOUR URGENT RESPOND.

FROM Mr.Kuso Acho.
The Head of File and Auditing Department, BANK OF AFRICA (B.O.A) Ouagadougou Burkina
(West Africa) REMITTANCE OF US\$20, 5;MILLION CONFIDENTIAL IS THE CASE. VERY URGE

ATTENTION

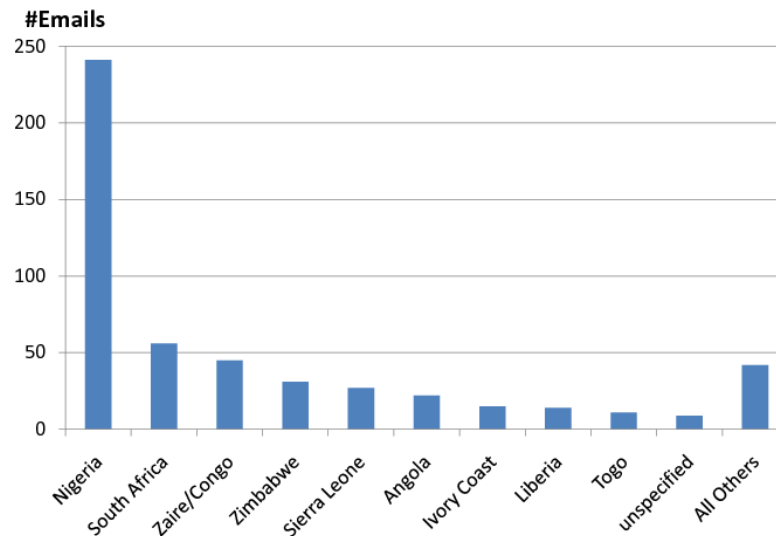
This message might meet you in utmost surprise, however, it's just my Urgent need for
partner that made me to contact you for this transaction I am a banker by profession
Burkina Faso in West Africa and currently holding the post of director Auditing and a
unit of the bank.

opportunity of transferring the left over Funds (\$20.5 million) of one
Along with his entire family in a plane crash.
you and me in this transaction will be deducted out
of the fund according to the percentages agr
transfer is over to receive my own share of
want you to understand that a stit
carry out this transaction with

Nigerian Emails:

Who falls for these things?

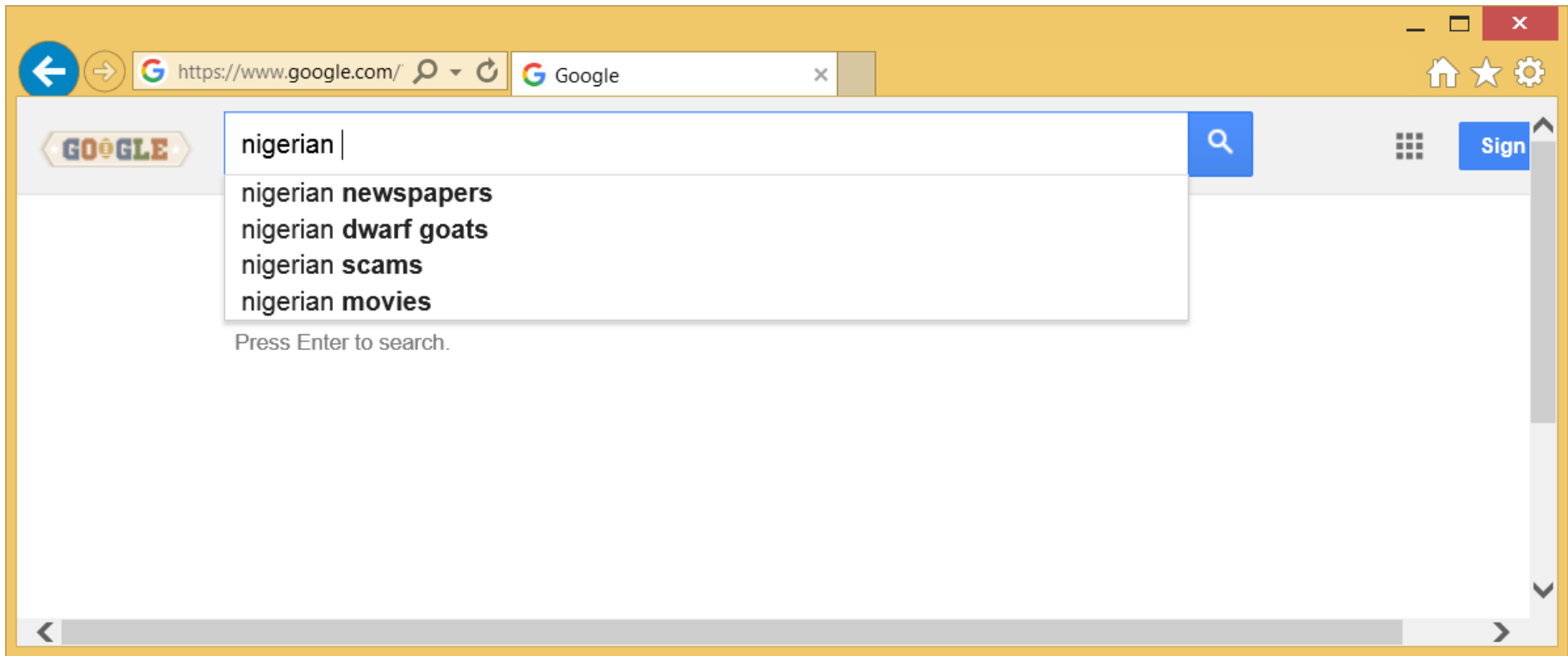
- What's with the spelling mistakes, BLOCK CAPS?
- Outlandish stories
- Why not Sweden, or Bolivia or New Jersey?



Nigerian Emails:

Who falls for these things?

- Who hasn't heard of [Nigerian Scam?](#)



- ***Ideally: attack only those who haven't heard of it.***


Ideally: attack only those who

- Will believe far-fetched story
- Haven't seen this before
- Won't use a search engine to check things out
- No family or friends who'll intercept
- Will transfer money to, e.g. Nigeria


What percent of population?

How do you find such people?

Send an email that repels everyone else


 Sat 9/12/2015 3:16 PM
Chantal Dubreuil <infogmbh@letgimenis.net>
Help me to invest EUR 12 million in your country?

To

 Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
This message was marked as spam using a junk filter other than the Outlook Junk E-mail filter.

Dear Sir,

I had worked as the technical advisor for my father his name is very well known as an ex-president of the republic. I would like to speak with international partners or private investors who have investment projects in which we can invest together with an important capital of 12 Million euros for a period of 20 years and he would be happy if this project can give us a net rate of return of 3.8% per year. If you have a project in which we can invest all of these funds, I am ready to work with you, but I preferred to entrust you all to the funds for a period of 20 years. If you have a good project in which you can help me to invest 12 Million euros, I am willing to give you a commission of 30%, equivalent 3.600.000 ₺ of these funds for the preparation of the project and its implementation. Once you start the project, you invest the balance 70% equivalent 8.400.00 ₺ in your project and you pay me the 3.8% net return per year for 20 years. Our joint partnership will be credible and official by the signing of a partnership contract between the two parties, and when this contract expires, you will repay me only the capital invested that is to say, the 8.400.00 ₺. If you have a special interest in this joint partnership, please contact me only through my private address: brigitteingaye@hotmail.com and we could discuss the whole process.

Chantal Dubreuil No Items 

Finding very rare targets

$$\text{Profit} = \text{\#successes} \times \text{Gain} - \text{\#fails} \times \text{Cost}$$

If $\text{\#fails}/\text{\#successes}$ too big, attacker makes a loss.

Two basic strategies:

- Attacker everyone
- Attack only very high-value targets

Attack everyone



Suppose:

- 1-in-1000 people use dog's name as bank pwd
- 10 mins/person to ***figure out*** dog's name.
- Average acct yields \$500

Congrats! Your yield is \$3/hour.

US wide this is a $200m \times \$500/1000 = \$100m$ opp.

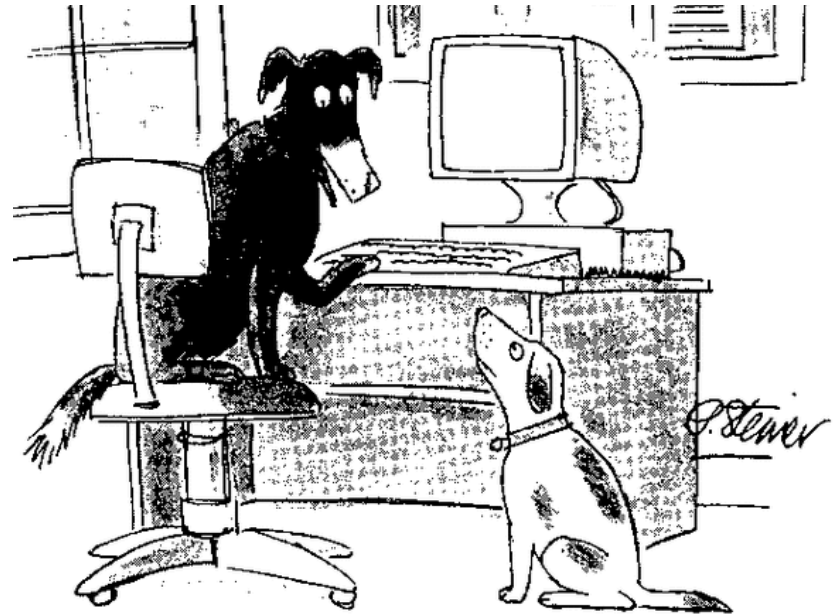
Can't afford any personalization:

- Must be ***fully*** automated

Attack only high-value targets

Value has to be visible:

- Celebrities
- Politicians



*“On the Internet, nobody knows you’re **not** a dog.”*

Higher than average visible value → worry
about targeted attacks

3. Sex, Lies and Cyber-crime Surveys

1 “ THE SHOCKING SCALE OF CYBERCRIME

PLAY AGAIN ▶

“ CYBERCRIME IS BIGGER THAN...



\$388 BILLION



...the global black market in **marijuana, cocaine and heroin** combined (\$288bn) and approaching the value of all **global drug trafficking** (\$411bn) i

431

At \$388bn, cybercrime is more than **100 times** the **annual expenditure of UNICEF** (\$3.65 billion) ii

1m+

SUMMARY: THE SHOCKING SCALE OF CYBERCRIME

THE TOTAL BILL FOR **CYBERCRIME** FOOTED BY ONLINE ADULTS IN **24 COUNTRIES** TOPPED USD \$388BN OVER THE PAST YEAR +



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



14

- Cybercrime estimates come from surveys

$$Estimate = \frac{|Pop.Size|}{|Sample.Size|} \sum_{i \in Sample} f[r_i]$$

- Surveys are reliable, right?
- Not when the errors don't cancel



A Curious Anomaly

Q: “How many sex partners of the opposite sex have you had?”

A: men report 5-10x higher than women.

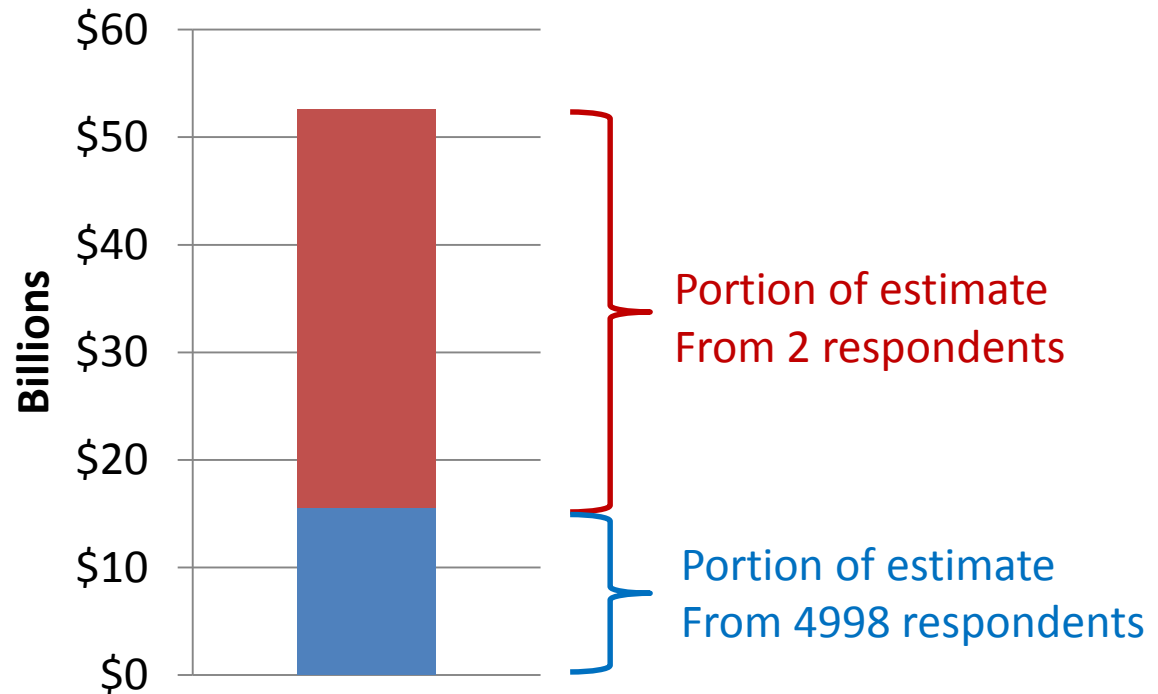
Not possible.

Morris '93: top 5% of male reports account for 85% of discrepancy

Bill Gates walks into a bar.....
average income goes up 1000x



FTC '06 ID Theft Survey: "Cybercrime cost \$52bn"



- Two respondents contribute \$37bn to estimate
- Two vote at 6000x strength of everyone else.

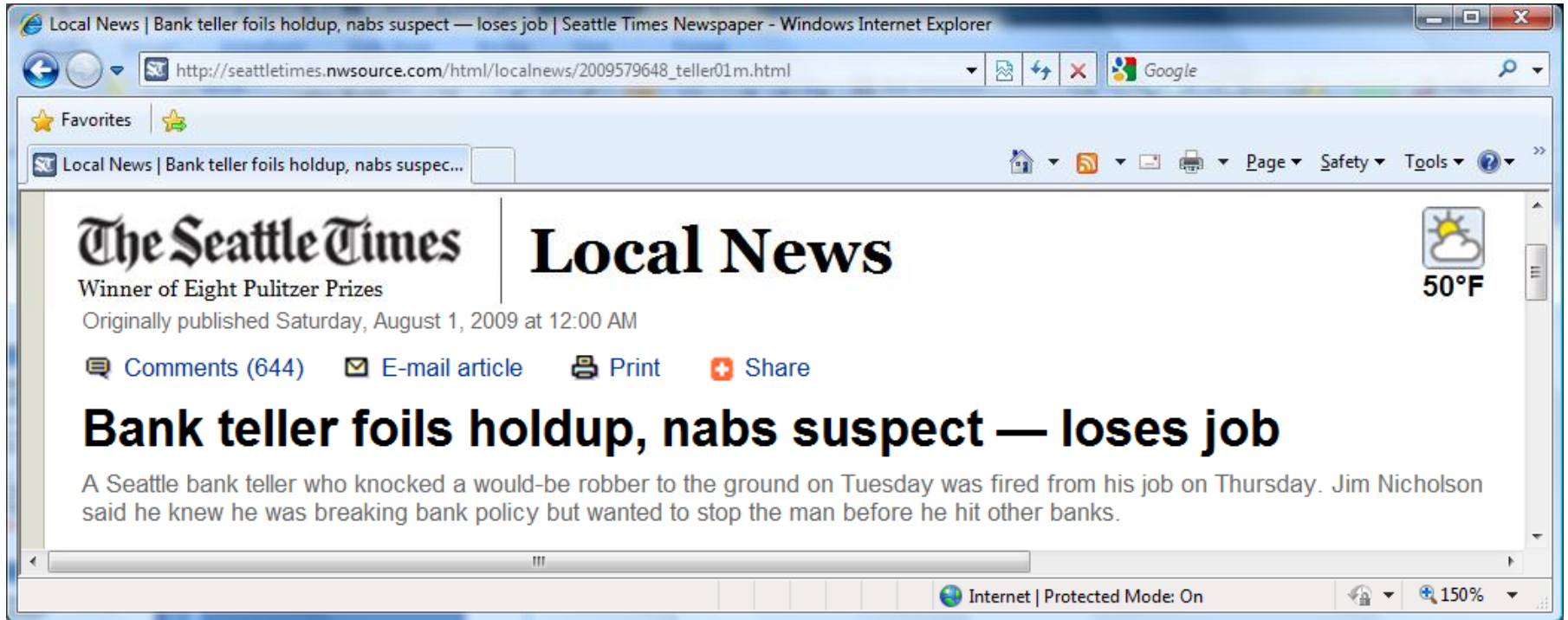
A 1000 person survey of #Pet Unicorns
in Ireland:



$$\begin{aligned} \textit{Estimate} &= \frac{|\textit{Pop. Size}|}{|\textit{Sample. Size}|} \sum_{i \in \textit{Sample}} f[r_i] \\ &= \frac{|4.5m|}{|1000|} \sum_{i \in \textit{Sample}} f[r_i] \end{aligned}$$

- **Every claimed unicorn adds 4,500 to estimate**

**4. Stealing passwords is easy,
getting money (and keeping it) is hard**



Banks understand:

1. Fear is bad for business
2. Getting money not the same as keeping it
3. Reversibility

My bank transfers money w/o password (or signature, or ID, etc)

American Express | Payment Center - Windows Internet Explorer

https://online.americanexpress.com/myca/onlinepayment/u santa cruz tax collector

Account Home | Statements & Activity | **Payments** | Profile & Preferences | Benefits | Additional Cards

BANK ACCOUNTS

Terms and Conditions | Need Help?

ENTER INFORMATION | VERIFY | THANK YOU

Enter your bank information

You are registering a new bank account for electronic payment services. Please have a paper check on hand for this process. You will need to enter and verify your financial institution's routing number and bank account number, which are located at the bottom of your paper check. When you've entered the required information, click "Continue".

Select bank account type :

Enter the 9-digit routing and transit number :

Enter the bank account number :

Re-enter the bank account number :

ROUTING AND TRANSIT NUMBER | ACCOUNT NUMBER

PLEASE NOTE:
You must use a checking account. Savings, money market, line of credit, credit and investment accounts, as well as balance transfer checks are not accepted.



Thief gets nothing if transfer is:

Detected



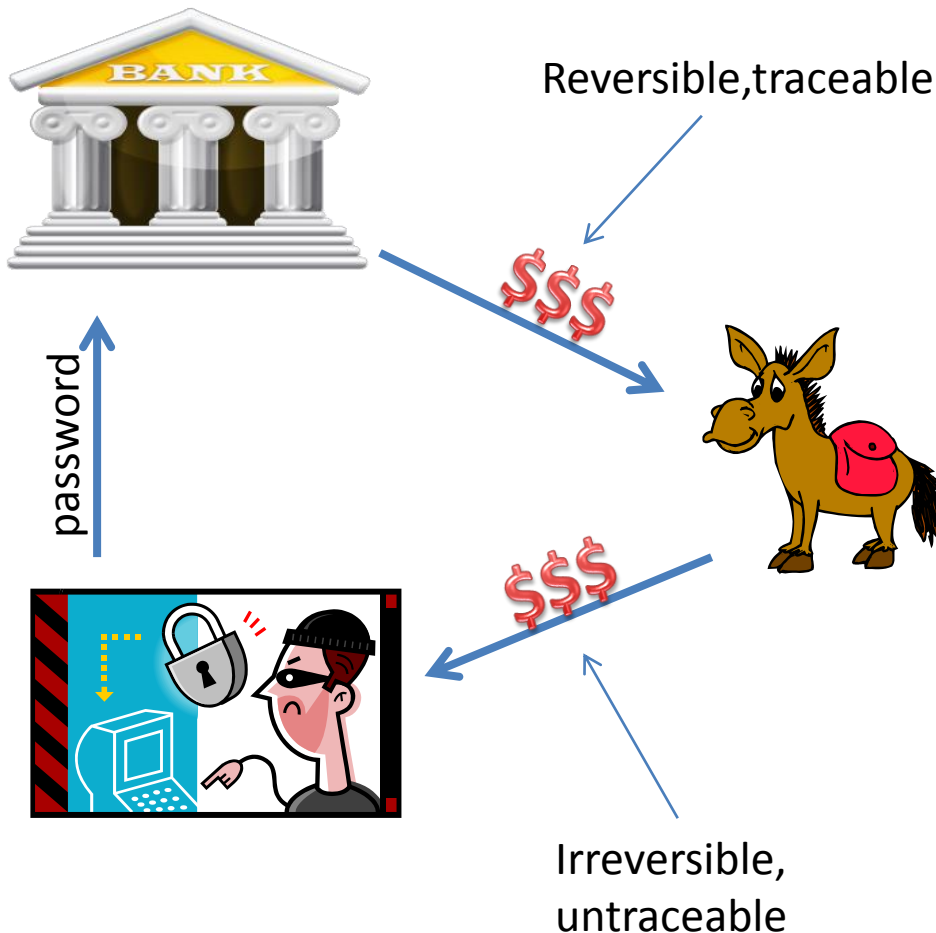
Reversed



Traced



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

The screenshot displays the LYDON ONLINE website, which provides Private Business Solutions. The interface includes a navigation menu with links for HOME, AGENTS, AWARDS, SOLUTIONS, and CONTACT US, along with a search bar. The main content area is titled 'Agent Preparation' and features a video player showing a man in sunglasses with the word 'Modification' overlaid. To the left of the video, there are three profile cards for staff members: Lance S. Turner (Division Manager), Shelly D. Daniels (Team Leader of the Quarter), and Jessica L. Howard (Agent of the Quarter). Below these are sections for 'Online Support Notifier', 'Private Messages' (no new), and 'Support Mailbox'. On the right side, there are three notification boxes: 'Agent Appreciation' (acknowledging agents), 'Staff Notice' (regarding meeting times), and 'Agent Notice' (regarding Team Leader positions).

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

A: Requires ID or signature on victim acct

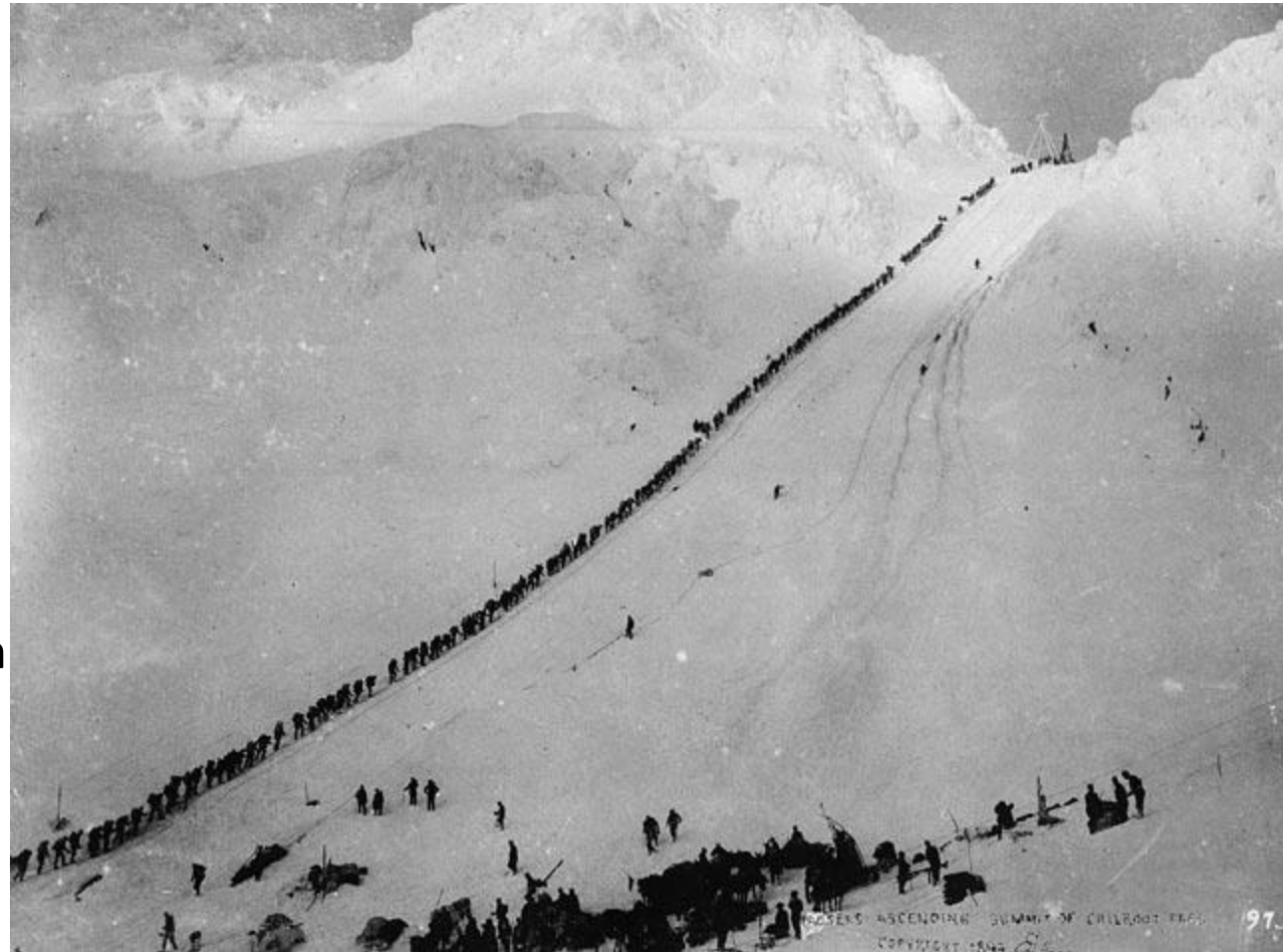
“But, they wouldn’t be doing it if they weren’t making money”



Effort \neq Dollars

Attempt to reach: 100,000
Reach Klondike: 20,000
Pan for gold: 12,000
Find any gold: 4,000
Get rich ($>$ \$5k): 300

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

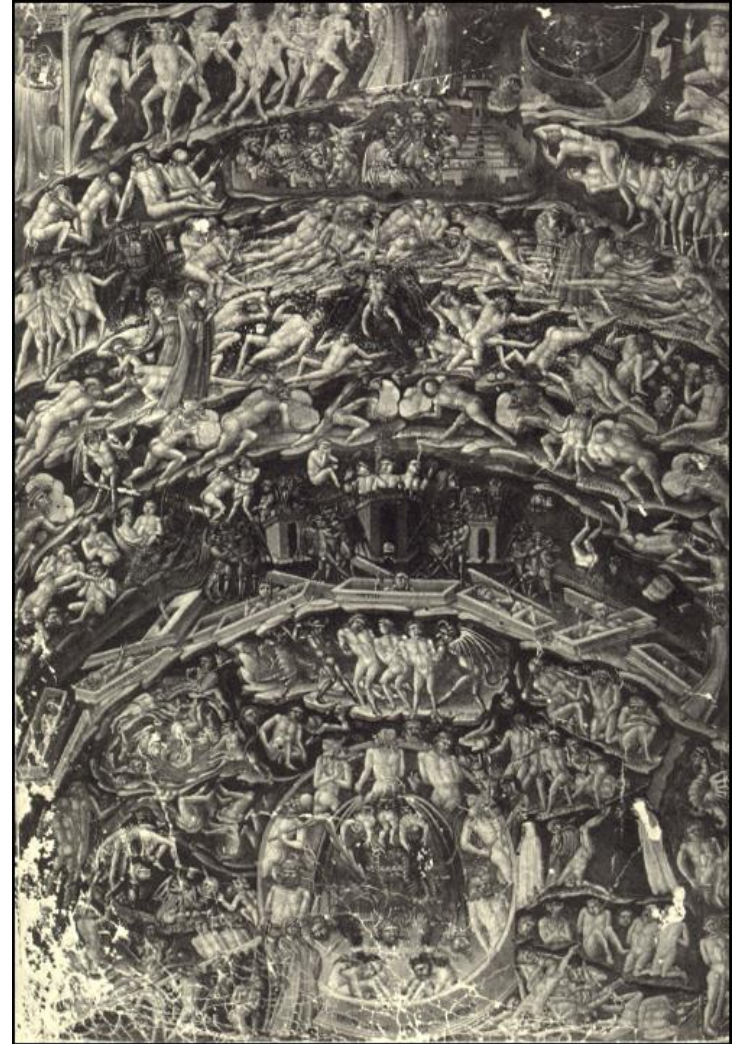


Prospectors on the way to the Klondike 1897

Serra Palada Goldmine, 1986



Dante's Inferno



“So it’s all no big deal then?”



ASHLEY MADISON®
Life is short. Have an affair.®

Get started by telling us your relationship status

Please Select

[See Your Matches](#)

Over 18,436,000 anonymous members!

The image shows a screenshot of the Ashley Madison website interface overlaid on a photograph of a woman's face. She has her index finger pressed against her lips in a universal gesture for silence or secrecy. The website text includes the brand name, a slogan, a form for relationship status, a 'See Your Matches' button, and a claim of over 18 million members.

Conclusions

- **Economics and Incentives**
 - Not every attack is economic
- **If it sounds too good to be true then it is**
 - Cyber-crime is not easy money
 - But that doesn't mean it's not a problem
- **We can reason about these things**
- **Don't be afraid.**

Supporting Documents

- ["Where Do Security Policies Come From?"](#), SOUPS 2010
- ["Why do Nigerian Scammers say they are from Nigeria?"](#), Proc. WEIS 2012
- ["Sex, Lies and Cyber-crime Surveys"](#), WEIS 2011
- ["Is Everything We Know about Password-Stealing Wrong?"](#), IEEE Security&Privacy magazine, to appear