Cybercrime & the Internet user:
If things are so bad how come they're so good?

Cormac Herley
Microsoft Research, Redmond
@cormacherley

Based on Joint work with Dinei Florêncio
$388 BILLION

The total bill for cybercrime footed by online adults in 24 countries topped USD $388bn over the past year.

Victims valued the time they lost to cybercrime at over $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).

At $388bn, cybercrime is more than 100 times the annual expenditure of UNICEF ($3.65 billion).
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 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 is believed to be growing at a CAGR of 1600% per year”

Scale, anonymity, action-at-a-distance
But they’re also pretty good
We all ignore most of this, and things still muddle along.
1. Where do security policies come from?
**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.

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

- **Username:**
- **Current Password:**
- **New Password:**
- **New Password (Repeat):**

If you need your password reset, but have
WA 520 Toll Bridge

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

<table>
<thead>
<tr>
<th>Sites</th>
<th>Median Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Traffic</td>
<td>19.9</td>
</tr>
<tr>
<td>Medium Traffic</td>
<td>19.9</td>
</tr>
<tr>
<td>Financial</td>
<td>31.0</td>
</tr>
<tr>
<td>Large Universities</td>
<td>44.5</td>
</tr>
<tr>
<td>Government</td>
<td>47.6</td>
</tr>
<tr>
<td>Accept adverts</td>
<td>19.9</td>
</tr>
<tr>
<td>No adverts</td>
<td>44.3</td>
</tr>
</tbody>
</table>

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

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: brigittesingaye@hotmail.com and we should discuss the whole process.
Finding very rare targets

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

If \#fails/\#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 x $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 $\rightarrow$ worry about targeted attacks
3. Sex, Lies and Cyber-crime Surveys
The Shocking Scale of Cybercrime

$388 Billion

The total bill for cybercrime footed by online adults in 24 countries topped USD $388bn over the past year.

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).

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

Victims valued the time they lost to cybercrime at over $274bn.

The direct cash costs of cybercrime - money stolen by cyberthugs/spent on resolving cyberattacks - totalled $114bn.
• Cybercrime estimates come from surveys

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

• 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:

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

\[ = \frac{|4.5m|}{|1000|} \sum_{i \in \text{Sample}} f[r_i] \]

- 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)
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”
  - Reversible
  - Traceable
- 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

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 ≠> 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
Serra Palada
Goldmine, 1986

Dante’s Inferno
“So it’s all no big deal then?”
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