Security Matters

Dr Richard Clayton
richard.clayton@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Digital Safety Conference
London, 19th June 2009

Outline

- It’s not just about children
- It’s not just about stupidity
- The limits of education
- What should users do ?
- What should the Government do ?

“Security” and “Safety”

- Standard words get used in precise ways – causing confusion
  - INTERNET — a connected network of networks
  - WEB — the subset of Internet hosts that have content
  - TRUST — a trusted component is one that has the ability to break your security policy
  - SECURITY — confidentiality, integrity and availability
  - SAFETY — not being hit on the head (even virtually)
- Silly words get invented – to make people look clever
  - SPAM — bulk unsolicited email
  - BLOG — a journal, or round-robin, placed on a web page
  - MALWARE — malicious software (including viruses and worms)
  - PHISHING — misappropriation of banking credentials
  - VISHING — phishing using automated telephone systems

and, regrettably, many more – some of which are in this talk

The real world

It’s not just cyberspace

- 2008: David Heiss, German online games player, developed a crush on Joanna Witton, and turned up outside her door in Nottingham… eventually murdering her partner Matthew Pyke
- 2008: Gary Grinhaff murdered estranged wife Tracey Grinhaff after she changed her Facebook page to say she was single

BUT these are the extremes of behaviour…

www.cosmogirl.com (Hearst Publications)

THE DAILY KISS BLOG

Today is Thursday June 18, 2009

search the daily kiss | SEARCH | search all the daily kiss topics | Select... | GO

‹ How to slow down and stay in love | daily kiss ▲ | Has a guy you've kissed ever made one of these make out mistakes? ›

filed in blog: the daily kiss, guys guide to guys

Dating 101: Online Stalking

November 3, 2008 at 12:00AM by **Kaitlyn Smith** | 20 comments

How often do you look at your ex-boyfriend's profile? If a girl writes on your crush's Facebook wall, do you immediately try to look at her profile to size up your competition? Have you memorized the interests and favorite movies of the cute boy in class — you know, the one you've never actually spoken to?

Little things like this done in a repeated fashion means you are becoming a bit obsessive and could be crossing into online stalker territory. Yes, the term "stalker" may be harsh. But there is a firm difference between casually glancing at your ex's MySpace and religiously analyzing every aspect of the Facebook page of some guy you have never spoken to.

How to Do It

There are some pretty sneaky ways to get the dirt on people — whether you are officially their "friend" or not.

-Subscribe to the blog of a total stranger. Does your crush have a blog? Subscribe to it! Then you can follow his day-

ADVERTISEMENT

about this blog

A blog about beauty, fashion, life, guys, and celeb news and gossip. read more ›

subscribe to this blog: email rss

about the authors

Deanne Hess	see all posts ›
Jessica Marati	see all posts ›
Megan Cahn	see all posts ›
Rose Walano	see all posts ›
Tammy Tibbetts	see all posts ›

categories

beauty | guys

What are cosmogirls being advised ?

- Use Facebook & MySpace to check for new friends for your “ex”
- Check who is writing on whose wall, and follow the conversation
- Google a person’s name to see what’s been written about them
- Join their regional network (because blocking is so complex)
- Create a new identity and befriend your ex
- AND “if you happen to know the password of an ex, or crush…”

- They do have some plausible advice:
  - check out the privacy options
  - be more careful about details
  - don’t give away your real birthday
  - though, strangely, no advice about changing your password

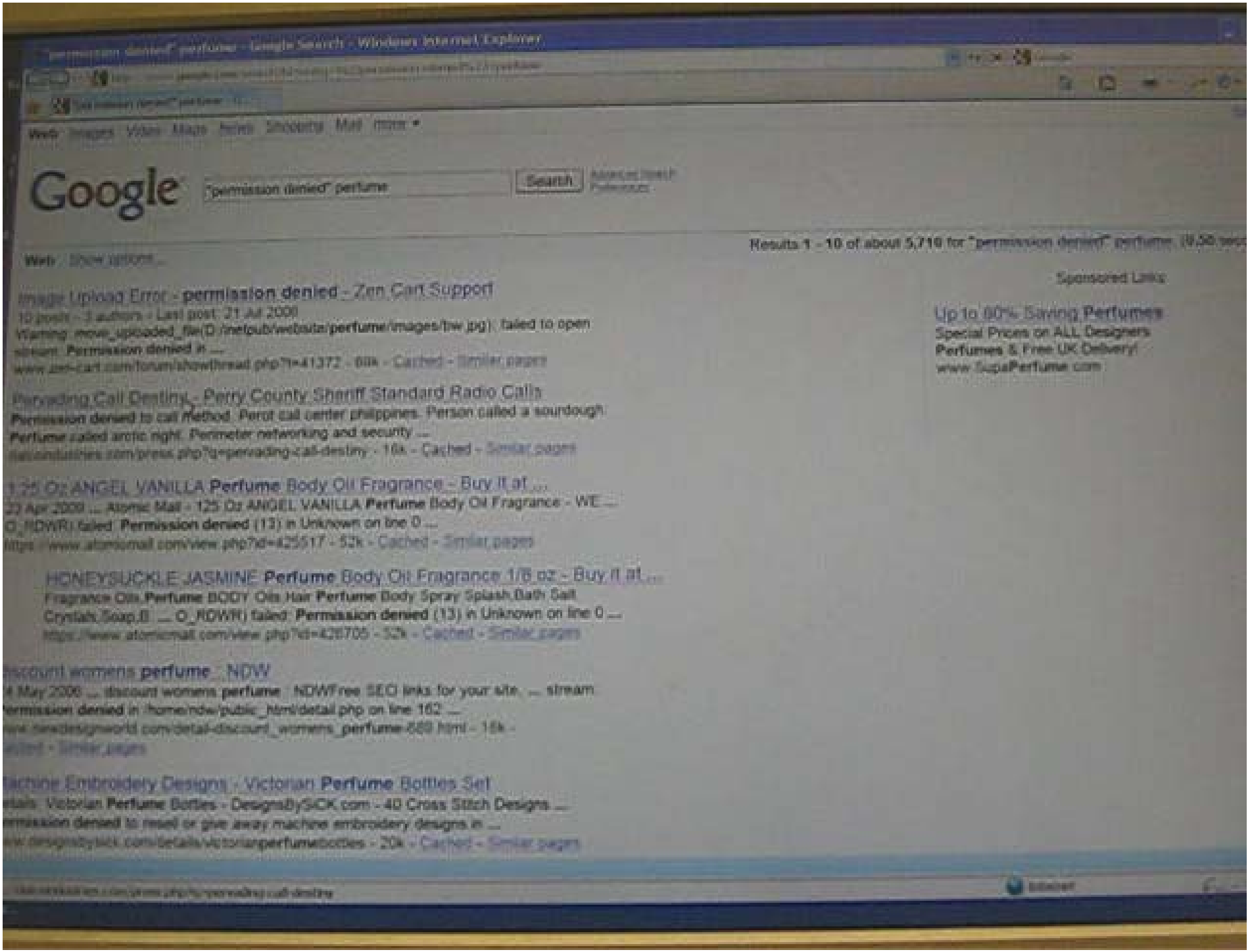
It’s not stupidity

Humans are good at persuading:

- 419 scams have been going on since forever
  - early 1900’s “Spanish prisoner” confidence trick
- A Ponzi scheme pays existing investors from new recruits
  - Dickens describes a scheme in Little Dorritt
  - Charles Ponzi said he was arbitraging international reply coupons
  - “women helping women” (Oct 2000), Albania (1995-7)
  - and of course, Bernie Madoff

URLs are too complicated for their own good:

- http://www.bankname.com@www.wickedness.com
- http://www.bankname.com.verysecure.com
- http://www.wickedness.com/www.barclays.com
- http://www.bankname.com.session1234567.wickedness.com
- http://www.bankname.com.%20%20%20%20%20%20%20%20%


Google
"permission denied" perfume
Search
Results 1 - 10 of about 5,710 for "permission denied" perfume
Sponsored Links
Up to 60% Saving Perfumes
Special Prices on ALL Designers
Perfumes & Free UK Delivery!
www.SupaPerfume.com
Image Upload Error - permission denied - Zen Cart Support
Pervading Call Destiny - Perry County Sheriff Standard Radio Calls
1.25 Oz ANGEL VANILLA Perfume Body Oil Fragrance - Buy it at ...
HONEYSUCKLE JASMINE Perfume Body Oil Fragrance 1/8 oz - Buy it at ...
discount womens perfume - NDW
Machine Embroidery Designs : Victorian Perfume Bottles Set

The limits of education

- It’s easy to explain how a lottery scam works
- It’s hard to explain how a URL is constructed
- It’s hard to explain how to judge whether an online virus scanner is a good thing to run, or a very major mistake
- BUT even an expert will fail to detect:
  - a keylogger
  - “man-in-the-browser” attacks
  - a router that accesses the wrong DNS server
  - poisoned DNS because your ISP is insecurely configured
  - incorrect BGP routing
  - forged CA certificates
  - etc etc

What can a mere user do ?

- ??? Run a virus checker ???
  - with a million new malware samples a month, it's rapidly becoming useless, but may save you when you click without thinking about it
- ??? turn on your firewall ???
  - rapidly becoming useless, because most of the difficulty arises with what goes out from your machine rather than what comes in; besides, the malware will just turn if off
- Patch and update everything you can
  - patch your operating system and all programs up to date
  - patch your router firmware up to date
- Change the default administration passwords on your ADSL/wireless router
- Never click on email links, but use your favourites menu

What is the “public policy” response

- We need to change the incentives surrounding security
  - ISPs must want to keep their users secure
  - manufacturers must ship “secure by default” equipment
- We must have better measurements
  - too many “statistics” are self-serving attempts to sell products
- We must make it more likely than not that a cybercriminal will be caught. The laws are in place, but enforcement is not
  - we’ve been here before: Bonnie & Clyde
  - we’ve been here before: Regional Crime Squads
- ePolicing needs to be revamped
  - we must increase international cooperation between police forces
  - we must fund more ePolice (perhaps not here, but in E Europe!)
  - we must pursue criminals across borders

Summary

- There are scary stories about murders, but what “cosmogirls” are doing is rather more significant
- There’s very significant limits as to how much we can fix through user education (but inquiries consistently recommend it, because it’s churlish to argue against it as a policy option)
- Instead we need to make the world safer by design
- Instead we need to catch and lock up more of the criminals
- Most of the lists of security advice are non-overlapping, inconsistent, wrong, dated and ineffective – but if you do one thing in June 2009 it should be to ensure that you are patching!

Security Matters

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory