

# Crime Science and Cyber Crime

Pieter.Hartel@UTwente.nl

# Contents

- Hypothesis
- Cyber Crime
- Crime Science
- Phishing Case Study
- Conclusions

# Hypothesis

Computer Science	Cyber Crime	Crime can break information security
Criminology	Crime Science	Crime can be prevented by opportunity reducing techniques
Multi-disciplinary	+	Opportunity reducing techniques can help to maintain information security

# Cyber Crime

- Old Crime is crime against:
  - » persons (e.g. rape, assault, murder, suicide)
  - » property (e.g. fraud, arson, theft, vandalism)
  - » the state (e.g. riot, treason, sabotage, terrorism)
  - » morality (e.g. gambling, drugs, obscenity)
- Cyber Crime is:
  - » Computer assisted crime ( $\approx$  Old Crime).
  - » Computer content crime (e.g. child pornography, identity theft, phishing, online auction fraud).
  - » Computer integrity crime (e.g. database theft, robbery at ATMs, and network integrity crime.)

[New09] G. R. Newman. Cybercrime. In M. D. Krohn, et al, editors, Handbook on Crime and Deviance. Springer, Nov 2009. <http://www.springer.com/978-1-4419-0244-3>

# Crime Science



[Cla97a] R. V. Clarke. Introduction. In R. V. Clarke, editor, Situational Crime Prevention: Successful Case Studies, pages 1-43. Harrow and Heston, 1997.

[http://www.popcenter.org/library/reading/PDFs/scp2\\_intro.pdf](http://www.popcenter.org/library/reading/PDFs/scp2_intro.pdf)

# Crime Science in a nutshell

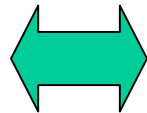
- Opportunity makes the thief
  - Crime is the product of choice +
- 
- Situational crime prevention:  
reduce opportunity to reduce  
crime
  - Crime specific focus!



# Situational crime prevention

## ■ Principles of situational crime prevention:

- » Increase effort
- » Increase risk
- » Reduce reward
- » Reduce provocation
- » Remove excuses



## ■ Design experiment

- » system, process, device...

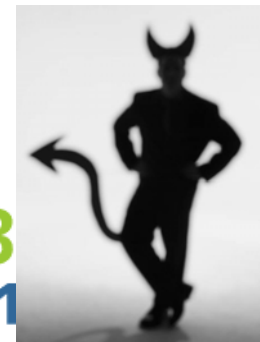
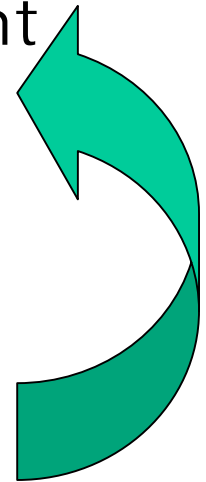
## ■ Implement

## ■ Evaluate

- » Efficiency
- » Effectiveness

## ■ Outcome

- » Diffusion of benefits
- » Reduction
- » **Displacement**



# 5×5 Opportunity reducing techniques

- Increase effort
  - » Time, skills
- Increase risks
  - » Of getting caught, failure, loosing resources
- Reduce rewards
  - » So that the offender has less benefits after the crime
- Reduce provocation
  - » So that the offender is less tempted to start
- Remove excuses
  - » So that the offender cannot justify the crime

[Wil09] R. Willison and M. Siponen. Overcoming the insider: reducing employee computer crime through situational crime prevention. Commun. ACM, 52(9):133-137, Sep 2009.

<http://dx.doi.org/10.1145/1562164.1562198>

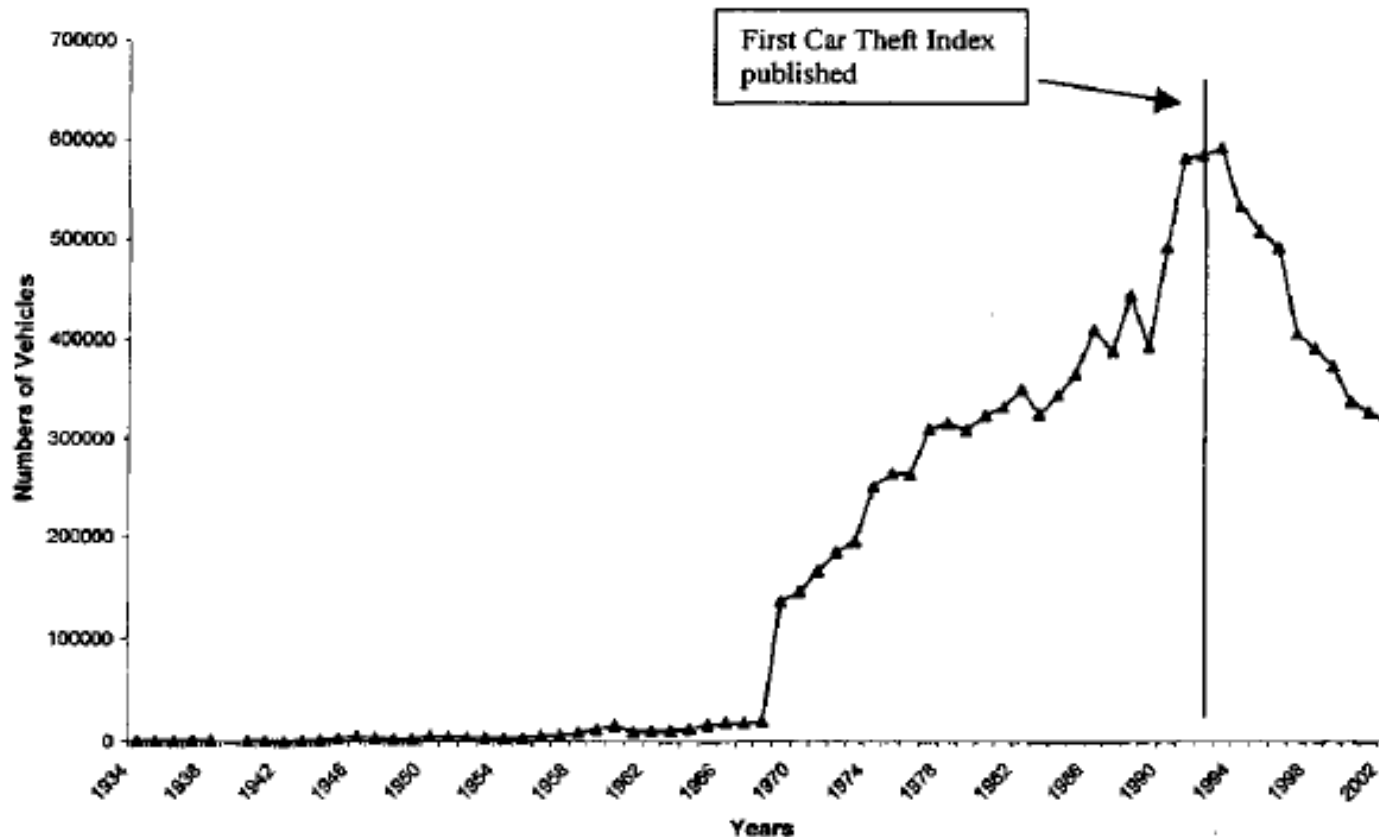
# Increase effort

1. Harden targets
  - » Firewalls; Steering column locks and immobilizers
2. Access control
  - » Caller ID; Electronic card access
3. Screen exits
  - » Audit logs; Ticket needed for exit
4. Deflect offenders
  - » Honey pots; Disperse pubs
5. Control tools & weapons
  - » Delete account of ex-employee; Smart guns



# A success story

**Figure 2: Number of Vehicles Stolen by Year**



[Lay04] G. Laycock. The UK car theft index: An example of government leverage. In M. G. Maxfield and R. V. Clarke, editors, *Understanding and Preventing Car Theft*, volume 17, page 2544. Criminal Justice Press, Monsey, New York, 2004.

[http://www.popcenter.org/library/CrimePrevention/Volume\\_17/03\\_laycock\\_webb\\_uk\\_car\\_theft.pdf](http://www.popcenter.org/library/CrimePrevention/Volume_17/03_laycock_webb_uk_car_theft.pdf)

# Phishing Case study

# What is phishing?

- Phishers try to get your sensitive info by masquerading as someone you trust
- Phishing is cheap and easy
- Phishing is lucrative
  - » Gartner group estimates losses of 2.8B\$ in 2009
- Phishers are hard to catch
- Victims are gullible

# How to reduce opportunity?

- Increase the effort
  - » Train users to be vigilant (more ...)
  - » Fill the database of the phishers with fake data
- Increase the risks
  - » Fill the database of the phishers with traceable data
  - » Revocable anonymity on phishing email
- Reduce Rewards
  - » ... ???

[Gaj08] S. Gajek and A.-R. Sadeghi. A forensic framework for tracing phishers. In 3rd IFIP WG 9.2, 9.6/ 11.6, 11.7/FIDIS Int. Summer School on The Future of Identity in the Information Society, volume 262, pages 23-35, Karlstad, Sweden, Aug 2007.

1 Springer, Boston. [http://dx.doi.org/10.1007/978-0-387-79026-8\\_2](http://dx.doi.org/10.1007/978-0-387-79026-8_2)

# Anti-phishing Phil

- [http://cups.cs.cmu.edu/antiphishing\\_phil/new/](http://cups.cs.cmu.edu/antiphishing_phil/new/)

**How To Avoid Online Scams**

Don't ignore the URL!

Looking at the address bar can help you figure out if a web site is legitimate or a scam!

Wombank

Accounts Contact About Us

Username:

Password:

login

http://143.127.22.13/wombank.html

The image shows a browser window with a blue header and a white body. The address bar is highlighted in orange and contains the URL 'http://143.127.22.13/wombank.html'. A blue callout box with a yellow arrow pointing to the address bar contains the text 'Looking at the address bar can help you figure out if a web site is legitimate or a scam!'. The page content includes the 'Wombank' logo, navigation links for 'Accounts', 'Contact', and 'About Us', and a login form with 'Username:' and 'Password:' labels, input fields, and a 'login' button. A cartoon orange fish wearing glasses is positioned at the bottom right of the callout box.

# Seven tips

1. Ignore email asking to update personal info
2. Ignore threatening email
3. Ignore email from bank that are not yours
4. Ignore email/url with spelling errors
5. Ignore url with ip address
6. Check url using Google
7. Type url yourself, don't click on it

[Dow06] J. S. Downs, M. B. Holbrook, and L. F. Cranor. Decision strategies and susceptibility to phishing. In 2nd Symp. on Usable privacy and security (SOUPS), pages 79-90, Pittsburgh, Pennsylvania, Jul 2006. ACM, New York.

<http://doi.acm.org/10.1145/1143120.1143131>

# A nice experiment

- 515 volunteers out of 21,351 CMU staff+stud.
  - » 172 in the control group, no training
  - » 172 single training, day 0 training
  - » 171 double training, day 0 and day 14 training
- 3 legitimate + 7 spearphish emails in 28 days
- No real harvest of ID

[Kum09] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. Blair, and T. Pham. School of phish: a real-world evaluation of anti-phishing training. In 5th Symp. on Usable Privacy and Security, pages 1-12, Mountain View, California, Jul 2009. ACM, New York. <http://doi.acm.org/10.1145/1572532.1572536>

# Results

- On day 0 about 50% of participants fell
  - » Constant across demographic
  - » Control group remains constant
  - » Single training reduces clicks
  - » Multiple training reduces clicks more
- People click within 8 hours of receiving the email(!)
- Unfortunately:
  - » Participants were self selected...
  - » No indication that this reduces crime...

# Risk for researchers

- Crawling social network site violates terms of service – use api, caches
- Copyright prohibits cloning web sites – work with the target, change the law
- Confusing trademarks damages good name of target – idem
- Phishing is illegal in California – avoid
- Make sure that your research is not in any way linked to commercial activities!

[Sog08] C. Soghoian. Legal risks for phishing researchers. In eCrime Researchers Summit, pages 1-11, Atlanta, Georgia, Oct 2008. IEEE.

<http://dx.doi.org/10.1109/ECRIME.2008.4696971>

# Current projects in Twente

- Study relation physical and IT security policies : laptop theft case
- Face recognition in images from surveillance cameras
- Study criminogenic properties of packaging designs with virtual reality
- Mapping of residential burglaries in Enschede
- Smart Tiles, light & sound to make the environment less inviting to crime

# Conclusions

- Crime Science approach
  - » Might have avoided experimental flaws
  - » Might have come up with new ideas
  - » Would have looked at crime prevention
- Crime prevention is a hard problem
- Disciplines must work together
- Many unexplored opportunities
- Twente would like to work on these problems with you...