Fight against Phishing

2007 AP* retreat Bali, Indonesia
February 25, 2007

Koichiro KOMIYAMA
Information Security Analyst, CISSP
JPCERT/CC (on behalf of APCERT)

Agenda

1. Global Trend of Phishing
   - Anti-phishing working group reports
2. Phishing in Japan
   - Based on reports to JPCERT/CC
3. Countermeasures
   - What can engineers do?
   - What can users do?

Global Trend of Phishing

Global Trend (part 1)

- Overview

  Increasing financial losses

  - According to a survey by Gartner, Inc., financial losses stemming from phishing attacks have risen to more than $2.8 billion in 2006.
  - 22,288 unique phishing URLs (per week) were found. (the U. S., 2006/10)
  - Phishing became so popular that it was listed in the Oxford English Dictionary.

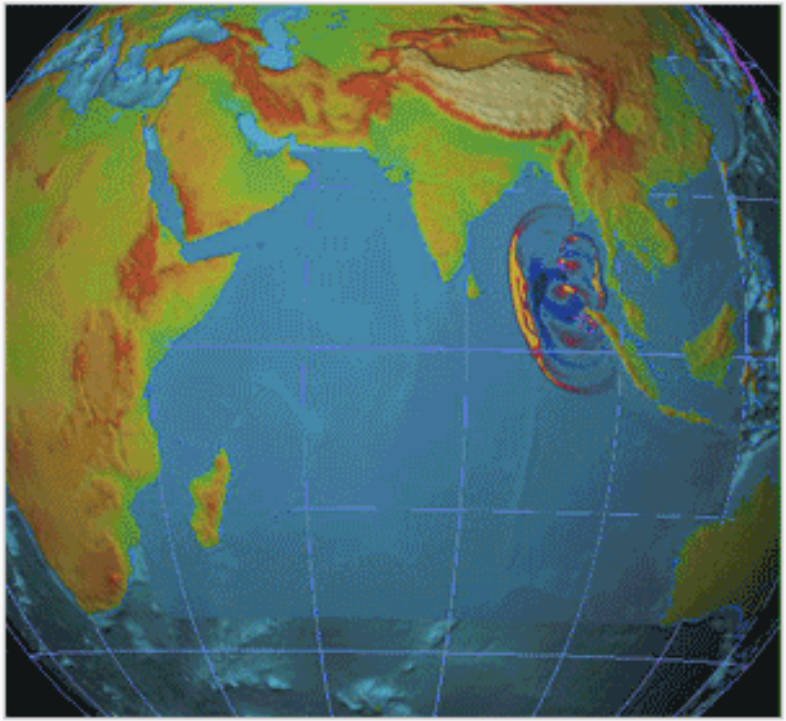
Global Trend (part 2)

- **April 2006**
  - 26 TLDs used to register fraudulent domains
  - 94% GTLDs (62% .com)
- **October 2006**
  - 36 TLDs used to register fraudulent domains
  - 49% GTLDs (10% .com)

Source: InternetIdentity

- **Phishers know the world isn't just .com.**
  - Low security/Slow response
  - Legal restrictions prevent take-down actions
  - E. g.) ncua.tk, northfork.de, wells-fargo.ws

Natural Disaster and Phishing (part 1)



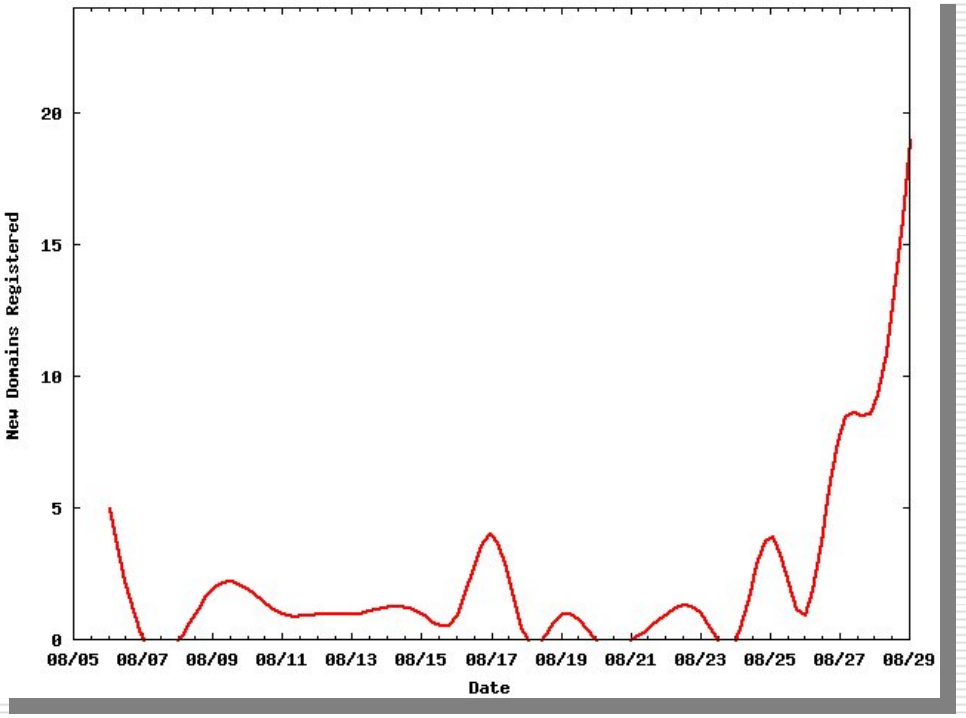
2004/12/26
A Tsunami caused by an earthquake of magnitude 9.0 hit Indonesia.

2005/1/5
FBI warned for scam tsunami aid websites.

2005/1/13
Arrest of a Pittsburgh man, an unemployed painter named Matthew Schmieder.

Natural Disaster and Phishing (part 2)

- In August 2006 domain names containing “Ernesto” (name of a hurricane that hit the U. S.) increased dramatically.

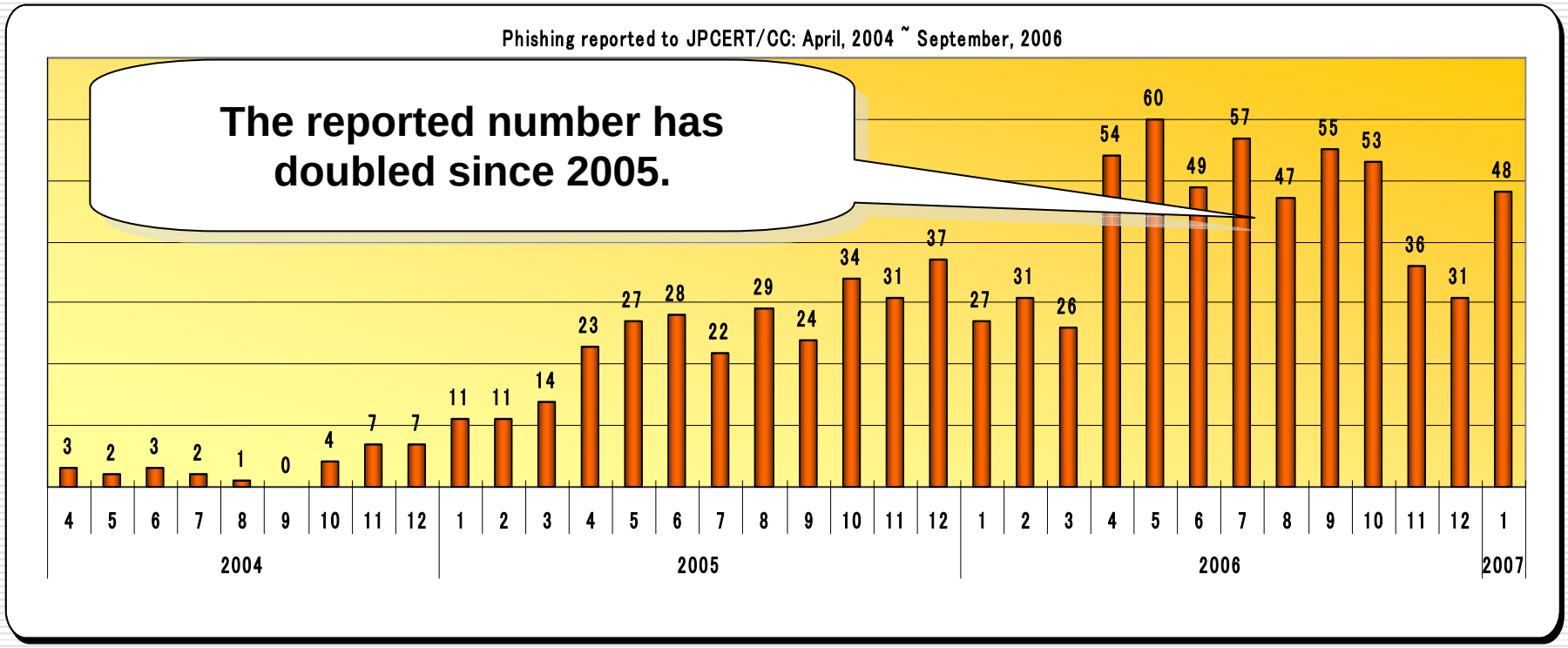


SANS Internet Storm Center
http://isc.sans.org/diary.html?storyid=1650

Phishing in Japan

Reports to JPCERT/CC

- Steady Inrease in the number of reports on Japanese servers used as phishing sites.



Two Type of Damages

Type A

- Victim: Web server owner
- Phisher: Compromises the web server and hosts a phishing site.

Type B

- Victim: Online service users/providers and brand owners (e.g., banking, payment, auction)
- Phisher: Acquire the owner's security sensitive information.

Phishing in Japan

- The Japanese internet users have not suffered major financial damages caused by phishing yet.
  - Language barrier
  - Only a few Japanese financial organizations offer online billing and communication to their customers.
  - The major target has been auction sites (no serious financial loss caused).

Advanced Techniques

- Wildcard DNS
  - **http://<any name>.example.com**
    - Allows practically infinite variations of the sites.
    - Put in your target brand name for credibility and style points.
    - Track your campaign's success – just like a real marketer DNS round robin.
- DNS Round Robin
  - hoshizora-bank.example.com -> multiple IPs
  - Uses a botnet
  - MUST kill the domain to stop the attack.

Summary

- Phishers are getting smarter.
  - The world isn't just ".com". Asia may be the next major target.
- Once phishing takes place, it is difficult to arrest the phishers.
  - Attacks are mainly from Russia, East Europe and China.
  - Phishers seem to be well organized.
  - Attacks are highly monetized.
- Taking down a phishing site is...,
  - Just a remediation, not a solution.

Effective countermeasures are required.

Countermeasures

Various Anti-Phishing Efforts

1. Prevent phishing site launches.
   - Take down phishing sites ASAP.
   - Prevent phishy domain names from being registered.
   - Establish websites that are difficult to mimic.
2. Reduce phishing mails
   - Anti-spam measures (OP25B, IP25B)
   - Sender domain Auth (SPF/Sender ID, DKIM)
   - Message signing (PGP, S/MIME)
   - Reduce bots (Anti-botnet project in Japan)
3. Countermeasures by the users
   - Use anti-phishing tools
4. Education

Prevent Phishing Site Launches

- Take down phishing sites immediately.
  - Need to improve our way of communication.
- Prevent phishy domain names from being registered.
  - Maintain a list of words that are most likely to be used as a phishing site's domain. (A registrar with a comprehensive list in the U. S.)
  - Share information of black-listed users.
- Establish websites that are difficult to mimic.
  - Login history
  - SSL Server Cert / EVSSL

Reduce Phishing Mails

- Reduce bot
  - Botnets are the main source of spam.
  - “Cyber Clean Center” project in Japan
    - https://www.ccc.go.jp/ccc/index.html

Reduce Phishing Mails

- Reduce spam
  - OP25B/IP25B
  - MAAWG (Messaging Anti-Abuse Working Group)
- Encourage to sign mail messages
  - PGP, S/MIME
- Sender domain Authentication (SPF/Sender ID, DKIM)
  - eBay and Paypal have already introduced SPF. DKIM will come shortly.

Countermeasures by the Users

- Anti-phishing tools
  - Freeware / browser plug-in
  - Two types of detection mechanisms
    - Database
    - Heuristic

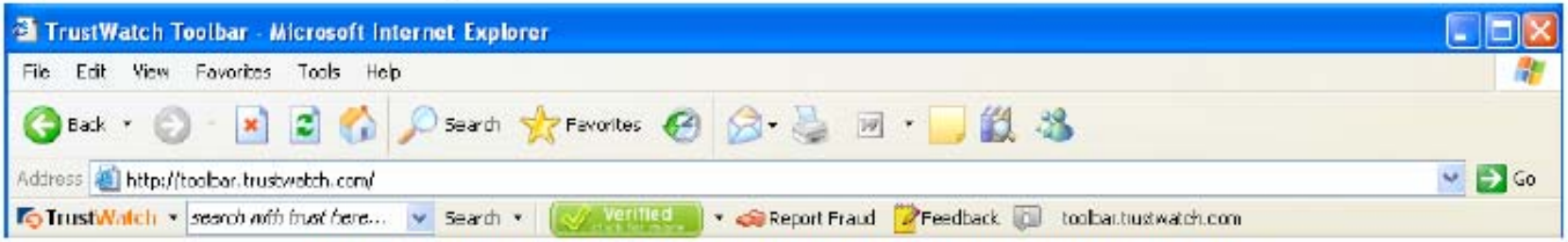


Figure 6: The GeoTrust TrustWatch Toolbar at a verified site.

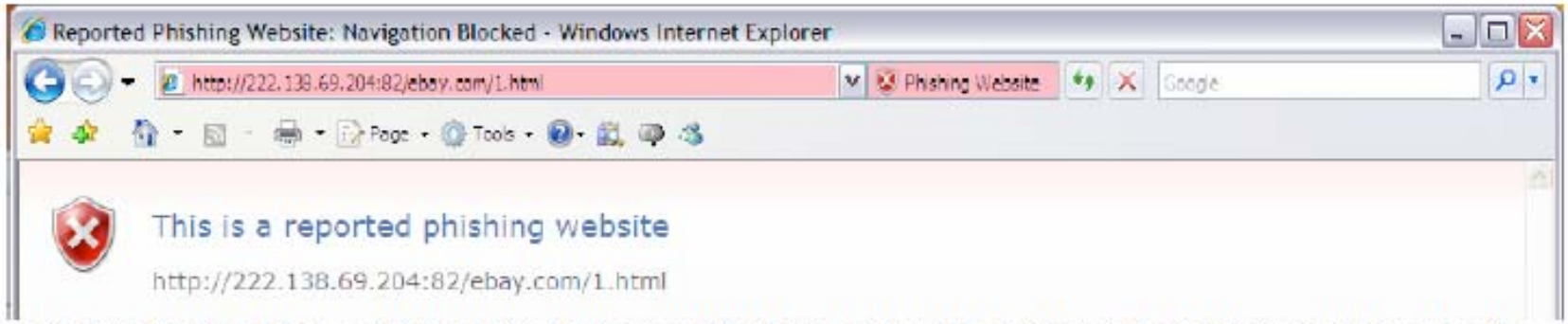


Figure 7: The Microsoft Phishing Filter in Windows Internet Explorer 7 at a fraudulent web site.

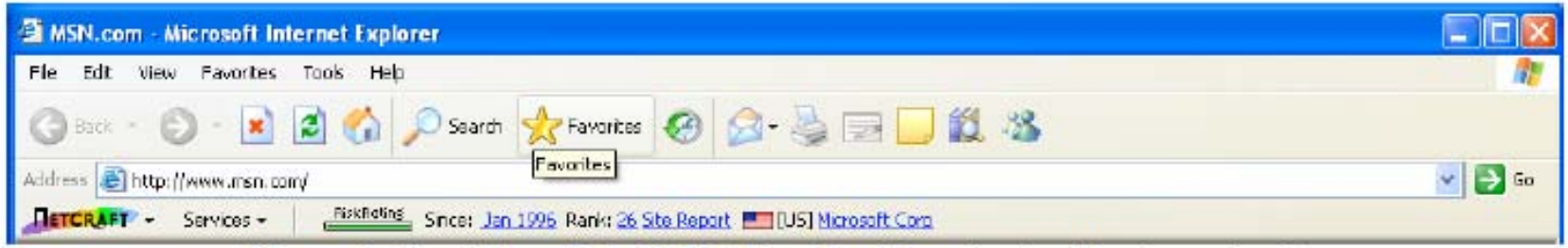
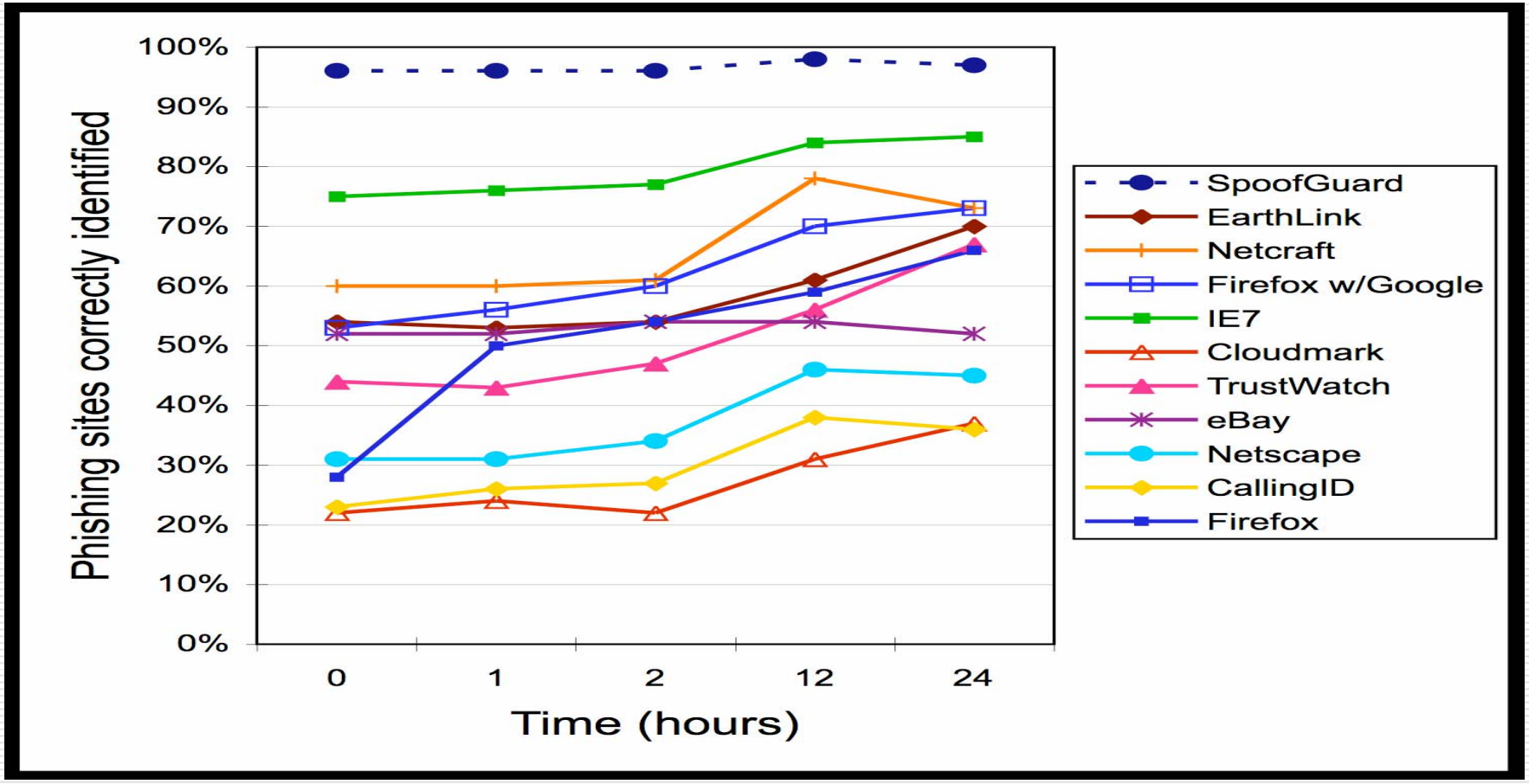


Figure 8: The Netcraft Anti-Phishing Toolbar at a legitimate web site.

出典: "Phinding Phish: Evaluating Anti-Phishing Tools" by Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong , 2007

Detection Rates



出典: "Phinding Phish: Evaluating Anti-Phishing Tools" by Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong , 2007

Various Types of Online Frauds

- **Phishing**
- Farming
- One-click fraud, two-click fraud
- Billing fraud
  - ”Transfer 400K yen to this account ASAP.”
  - Send a mail that looks like a payment order from the district court.
- Vishing
- **Pump and dump**
  - Send a mail recommending the receiver to purchase a specific stock. When the specific stock becomes a gainer, sells off his/her stock before its price drops. It is said that pump and dump makes up 15% of the spam.
- Counterfeit security software
- **Fraud within the online game world (abuse RMT)**
- **Internet auction fraud**
- **Affiliate fraud**
  - Increase the number of clicks fraudulently through a program.

Must have the whole picture of online frauds to take effective countermeasures against phishing.

Summary

- Passive -> Pro-active
- The issue shall not be solved only through technology.
- Must have the whole picture of online frauds.
- User education is always the essential part of the solution.
  - Always keep your brain updated by applying a patch named “education”!
- What JPCERT/CC does:
  - Take down phishing sites in Japan.
  - Education
  - May be it is time to shift the focus from “phishing” to “online fraud”?

Questions?

- Contact JPCERT/CC
  - Email: office@jpcert.or.jp
  - Tel: +81-3-3518-4600
  - http://www.jpcert.or.jp/

- Report Phishing

  info@jpcert.or.jp

JPCERT/CC is an independent non-profit non-governmental organization, acting as a national point of contact for the other CSIRTs in Japan. Since its establishment in 1996, the center has been gathering computer incident and vulnerability information, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues. JPCERT/CC is sponsored by the Ministry of Economy, Trade and Industry.

Appendix

- Appendix1: One-Click Fraud
- Appendix2: Social Phishing
- Appendix3: Billing Fraud

Appendix 1: One-Click Fraud

1, One receives a SPAM e-mail with a URL.

2, There is a simple “Enter” button.

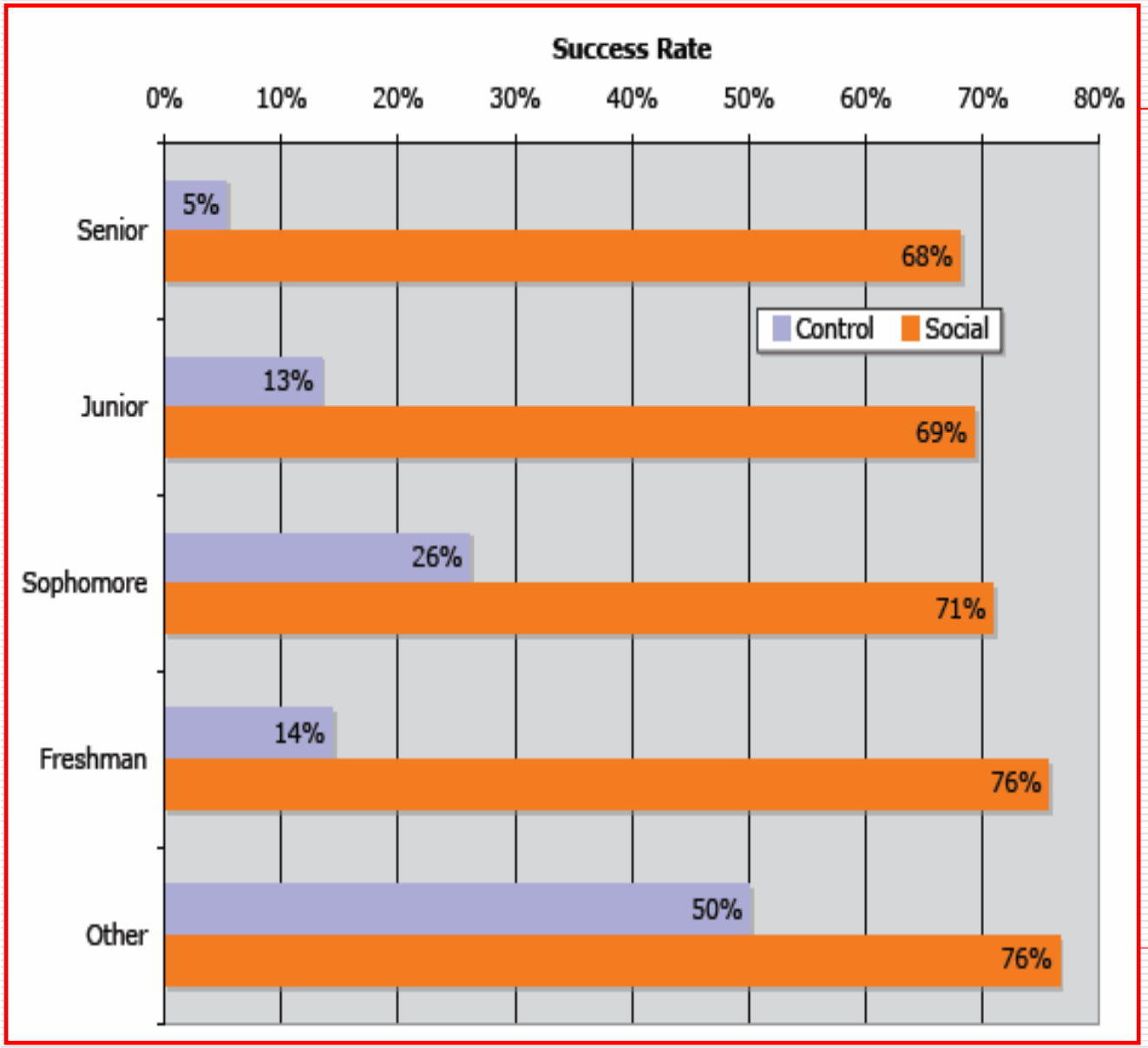
3, “You MUST pay 10,000 Yen within xx days….”

Appendix2: Social Phishing

- インディアナ大学で2005年12月に行われた実験
  - 学生900名にフィッシングメールを送りつける
  - ソーシャルエンジニアリングを使うと攻撃成功率が4倍に。
  - フィッシング＋ソーシャルエンジニアリング
    - myspace.com, facebook.com, eBay

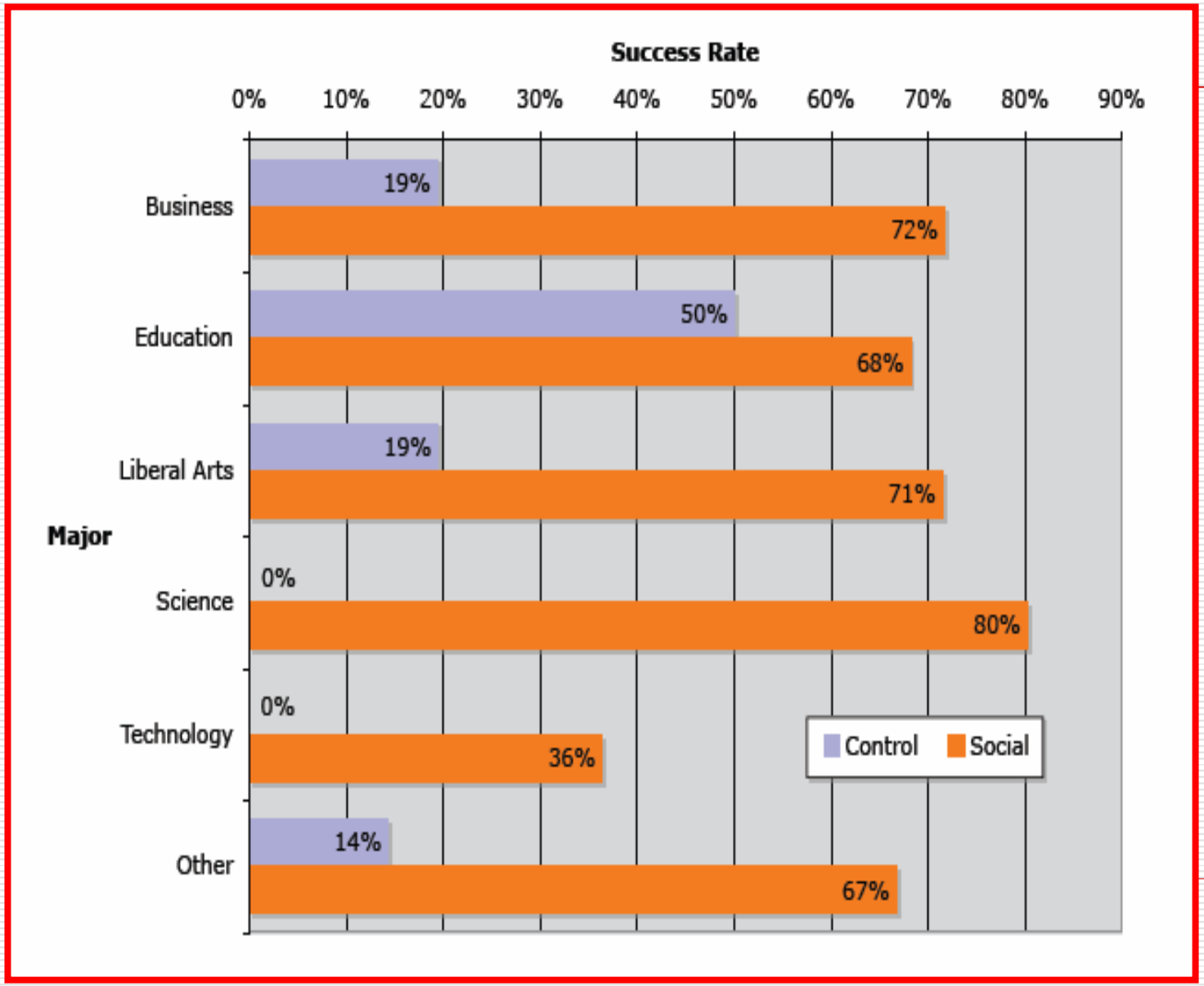
出典: Social Phising, Indiana University (Dec 12, 2005)
http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

Freshman, easy to phish.



出典: Social Phising, Indiana University (Dec 12, 2005)

Science, know much about technology, but vulnerable



出典: Social Phising, Indiana University (Dec 12, 2005)

性差

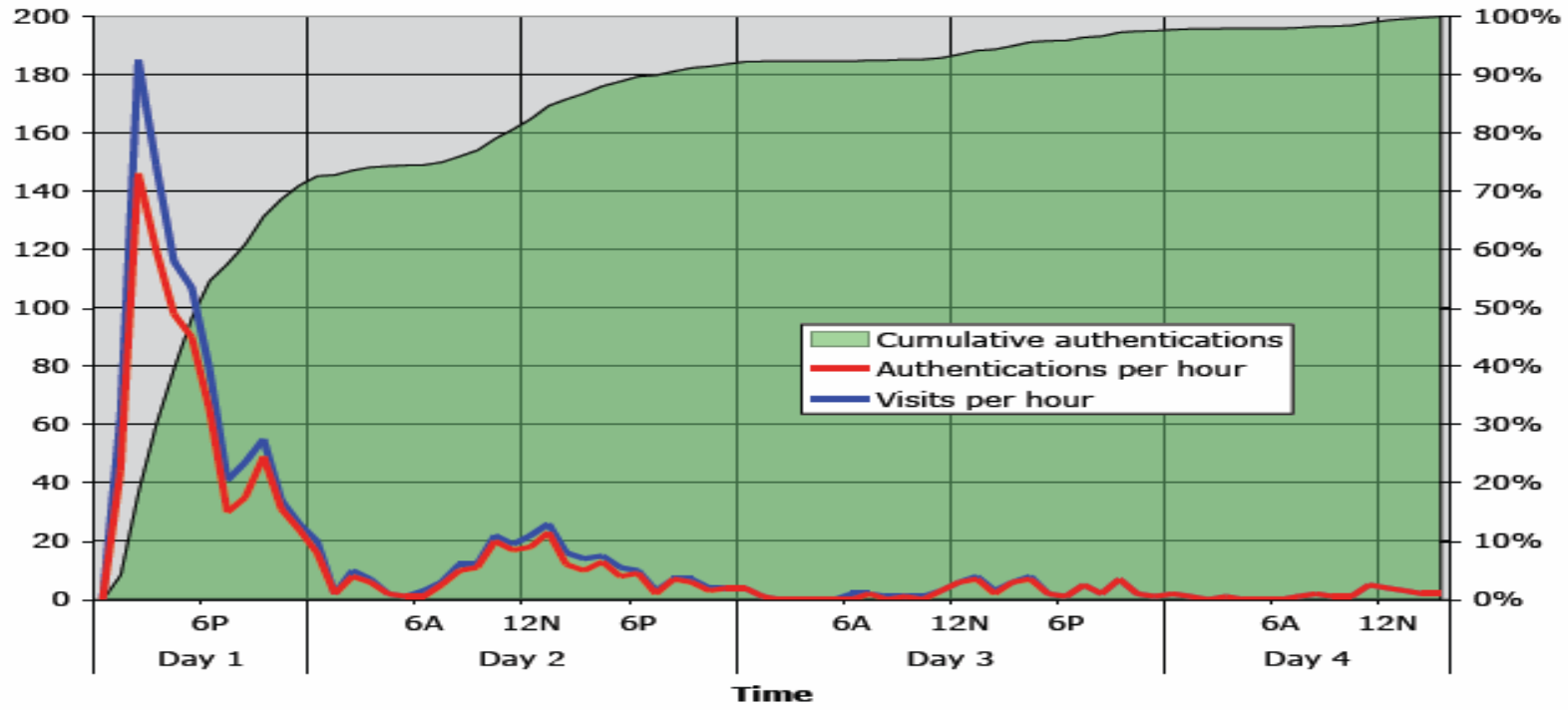
- 男性 → 男性
  53%
- 女性 → 男性
  68%
- 男性 → 女性
  78%
- 女性 → 女性
  76%

- 女性の方が被害にあう確立が高い
- 異性からのメールは魅力的？

出典: Social Phising,
Indiana University (Dec 12, 2005)

Action should be taken within 12h

- 被害の70%は最初の12時間で起こっている



出典: **Social Phising, Indiana University (Dec 12, 2005)**
http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

Appendix3: Billing Fraud

- Billing fraud is a type of social engineering. The attacker shows a hoax billing page.
  - Fakeware
  - One-click fraud
  - Two-click fraud
- Most of the Japanese cell-phones can access the Internet; thus the cell-phone users are also vulnerable.
- Billing fraud is the most popular online fraud since it is easier than launching a phishing site.