IT-Security 1

Chapter 10: Phishing

Prof. Dr.-Ing. Ulrike Meyer

WS 15/16

Chapter Overview

- What’s ‘classical’ phishing?
- Trends in phishing
- How is it done?
  - Ways to make users follow a link to a faked website
  - Making URLs of fake websites more believable
  - Ways to make users belief that a website is real
  - Ways to bring fake websites online
- Protecting against phishing
- How serious is phishing?
- References

What’s Phishing?

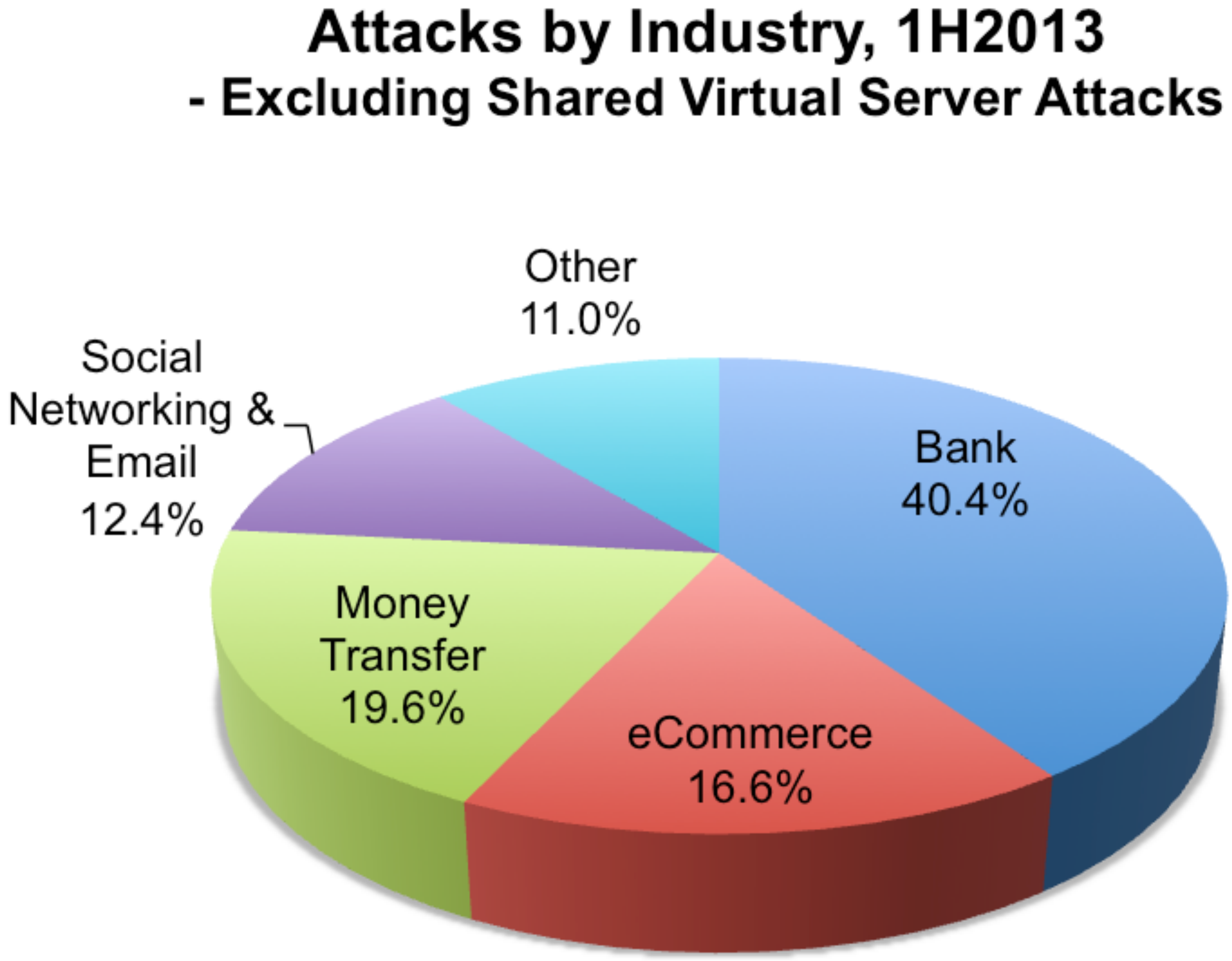
- ‘Classical’ Phishing
  - Victims are sent emails (or other electronic messages)
  - That deceive them into providing account numbers, passwords, credit card numbers or other personal information to an attacker
- Typically, emails claim to originate from a reputable business where the victim may have an account
- Email contains link to spoofed website where victim enters the personal information
- The word "phishing" comes from the analogy
  - that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users
  - Note that "Ph" is a common hacker replacement for "f“
- Phishing thus applies both
  - Social engineering and technical subterfuge

Subcategories

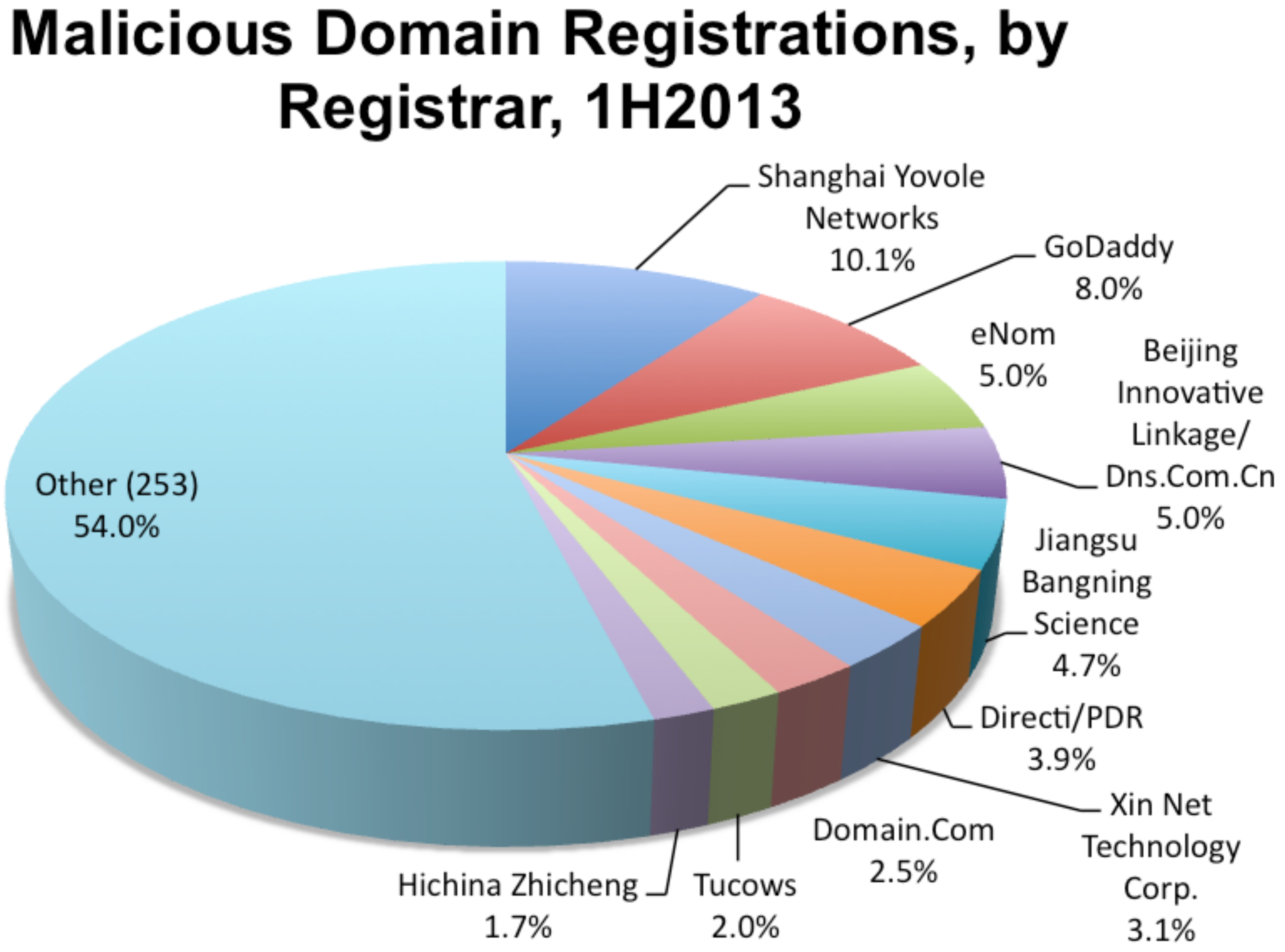
- Spear phishing
  - Phishing attacks directed against a particular (group of) user(s)
    - E.g. send phishing emails from local bank to students enrolled in local university
    - Send phishing emails addressing the victim personally

- Whaling:
  - Phishing attacks targeted at senior executives of companies or political leaders

Phishing Reports [APWG]



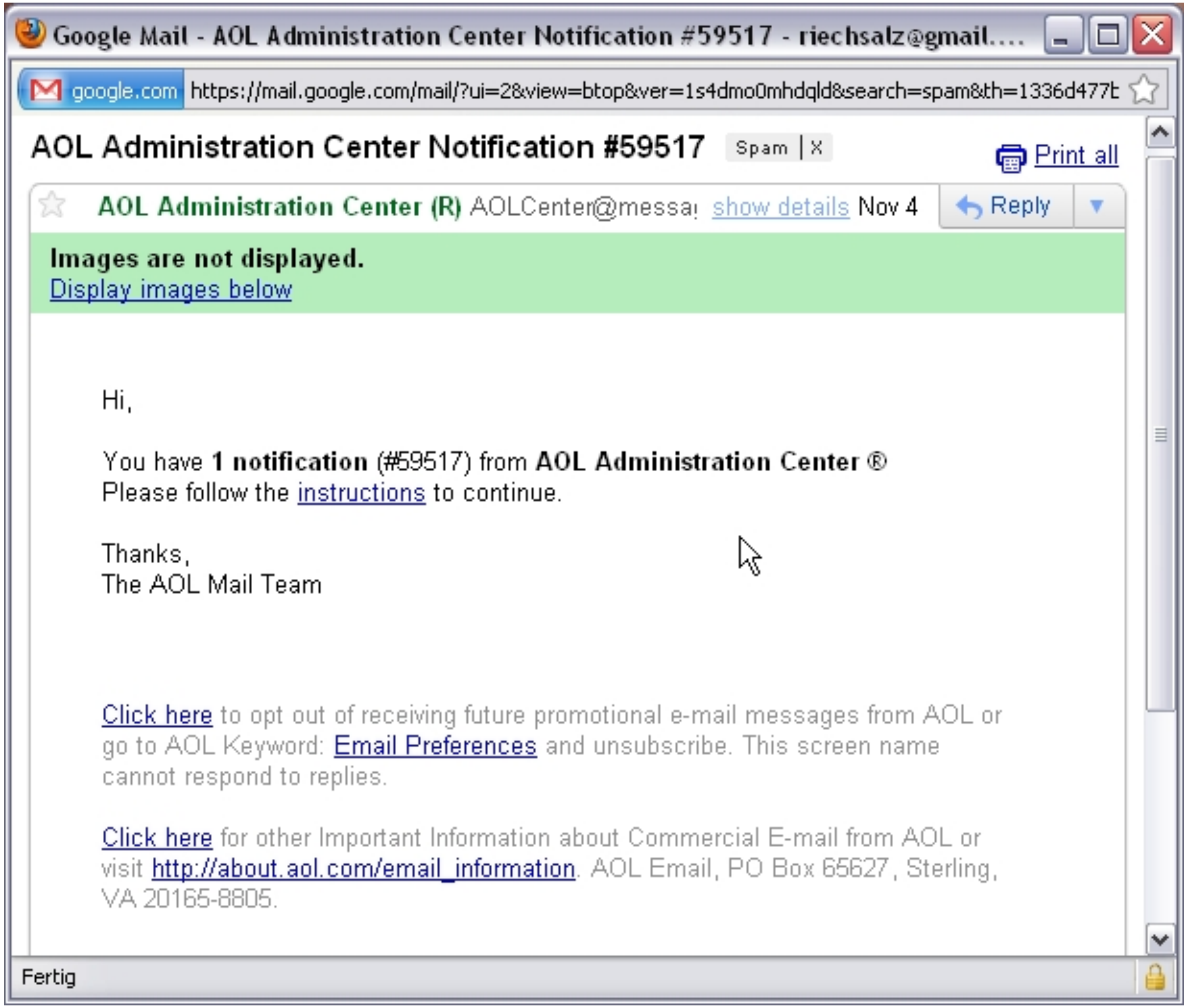
Phishing Reports [APWG]



Ways to Make Users Access a Particular URL

- Links in emails
  - Classical Phishing emails claiming to come from a legitimate source like your bank etc.
  - Including a link to a faked web site
- Links in instant messages
  - E.g. 2006: computer worm took over pages on MySpace
    - Sent instant messages to other people in contact lists including link to spoofed MySpace login page
    - After entering login data people were redirected to real page
    - Attacker obtained login data this way
- Links in short messages
  - Sometimes called SMiShing

Example: Phishing Email



Google Mail - AOL Administration Center Notification #59517 - riechsalz@gmail....
google.com
https://mail.google.com/mail/?ui=2&view=btop&ver=1s4dmo0mhdqld&search=spam&th=1336d477b
Print all
Spam | X
show details
Reply
Fertig

AOL Administration Center Notification #59517

AOL Administration Center (R) AOLCenter@messa Nov 4

Images are not displayed.
Display images below

Hi,

You have **1 notification** (#59517) from **AOL Administration Center ®**
Please follow the instructions to continue.

Thanks,
The AOL Mail Team

Click here to opt out of receiving future promotional e-mail messages from AOL or go to AOL Keyword: Email Preferences and unsubscribe. This screen name cannot respond to replies.

Click here for other Important Information about Commercial E-mail from AOL or visit http://about.aol.com/email_information. AOL Email, PO Box 65627, Sterling, VA 20165-8805.

Taking a Closer Look

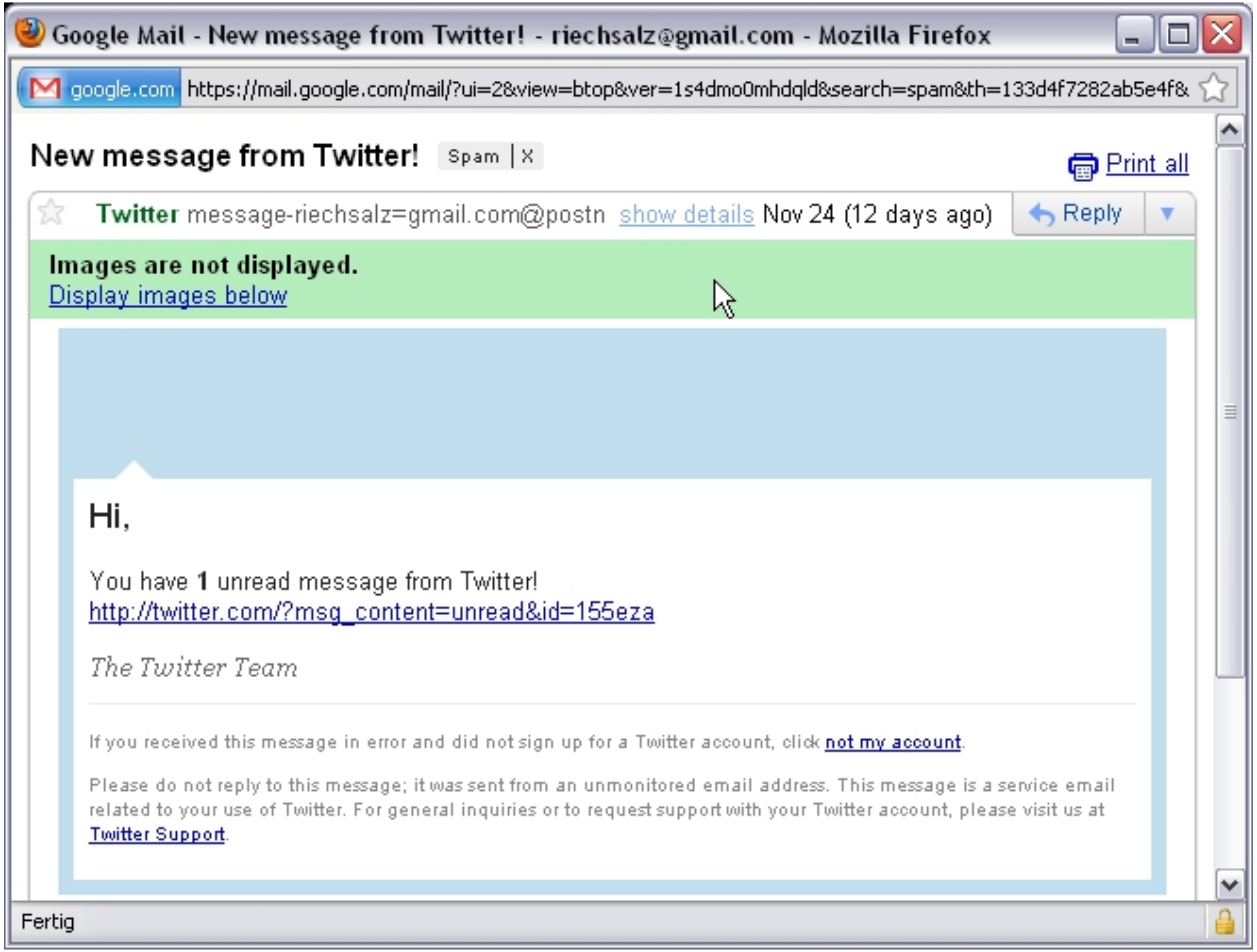
- You have **1 notification** (#59517) from **AOL Administration Center ®**

  Please follow the instructions to continue.

  Thanks,
  The AOL Mail Team

  Click here to opt out of receiving future promotional e-mail messages from AOL or go to AOL Keyword: Email Preferences and unsubscribe. This screen name cannot respond to replies.

Example: Phishing Email



Google Mail - New message from Twitter! - riechsalz@gmail.com - Mozilla Firefox
google.com https://mail.google.com/mail/?ui=2&view=btop&ver=1s4dmo0mhdqld&search=spam&th=133d4f7282ab5e4f&
Print all
Reply
show details
Fertig

New message from Twitter! Spam | X

Twitter message-riechsalz=gmail.com@postn Nov 24 (12 days ago)

Images are not displayed.
Display images below

Hi,

You have **1** unread message from Twitter!
http://twitter.com/?msg_content=unread&id=155eza

The Twitter Team

If you received this message in error and did not sign up for a Twitter account, click **not my account**.

Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of Twitter. For general inquiries or to request support with your Twitter account, please visit us at Twitter Support.

Looking closer…

Hi,

You have **1** unread message from Twitter!
http://twitter.com/?msg_content=unread&id=155eza

The Twitter Team

If you received this message in error and did not sign up for a Twitter account, click not my account.

Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of Twitter. For general inquiries or to request support with your Twitter account, please visit us at Twitter Support.

Example: Phishing Email

From: survey@survey.chase.com
To: Recipient
Sent: 11/21/2008 8:17:54 A.M. Eastern Standard Time
Subject: Customer Satisfaction Survey
Dear Chase client,
Due to the rumors of financial crisis, Chase has decided to make a nationwide
survey. The information collected will be used to improve our services and your
banking experience with us.
For the completion of this survey, we will credit your account with $100.
To take part, please click here.
Note - The information we gather from this survey will not be handed down
to any third party.
© 2008 JPMorgan Chase & Co.

And One More from My Inbox

Dear Valued Customer,

Online security - The steps we take

Ensuring your online transactions are safe and secure

As a bank we are used to thinking about security. The growth of the internet has offered greater flexibility for us all, but it also brings new risks that must be guarded against. At HSBC, we use industry standard security technology and practices, focusing on three key areas privacy, technology and identification to safeguard your account from any unauthorized access.

Online security - The steps you should take

There is much that you can do to protect yourself online. Some of these measures are simple, others may require a little time invested or following simple instructions sent by us to you by email, Phone or Post. As part of our security measures, We are introducing Secure Transact, one of the various security initiatives we are introducing this Year. To enroll in Secure Transact please click on the LOG IN button below. This Email has been sent to all HSBC Bank Customers, Failure to follow the Enrollment process properly will result in account suspension for security reasons

More sophisticated Ways to Make Users Access a Particular URL

- Domain Name Resolving Attacks
  - Using DNS cache poisoning, i.e. injection of wrong information into DNS query response that will be cached by the requesting resolver
  - Add malicious entries to a computer's 'hosts' file that will be checked by the local domain name resolver before making a request to a DNS server
- Cross-Site Scripting Attacks
  - Web sites that accept user input are potential vulnerable to this
  - E.g. a phisher could construct a URL that uses a vulnerable program on a legitimate commerce site
  - The URL could contain code such as code in JavaScript that could target account credentials

Making Fake URLs More Believable (1)

- Use confusing URLs
  - http://paypal.accounts.com
- Use URL with multiple redirection
  - http://www.chase.com/url.php?url="http://phish.com"
- Register similar URLs or URLs with typos
  - http://www.paypai.com or even better http://www.paypaI.com using a capital 'i'
  - http://www.e-bay.com
  - http://www.rur-uni-bochum.de
  - http://www.tu-darmstad.de/
- Use alternate encoding schemes for URLs
  - Hexadecimal encoding instead of ASCII Text or the dotted quad representation of IP addresses
    - E.g.%68%74%74%70%3a%2f%2f%77%77%77%2e%65%78%61%6d%70%6c%65%2e%63%6f%6d = http://www.example.com

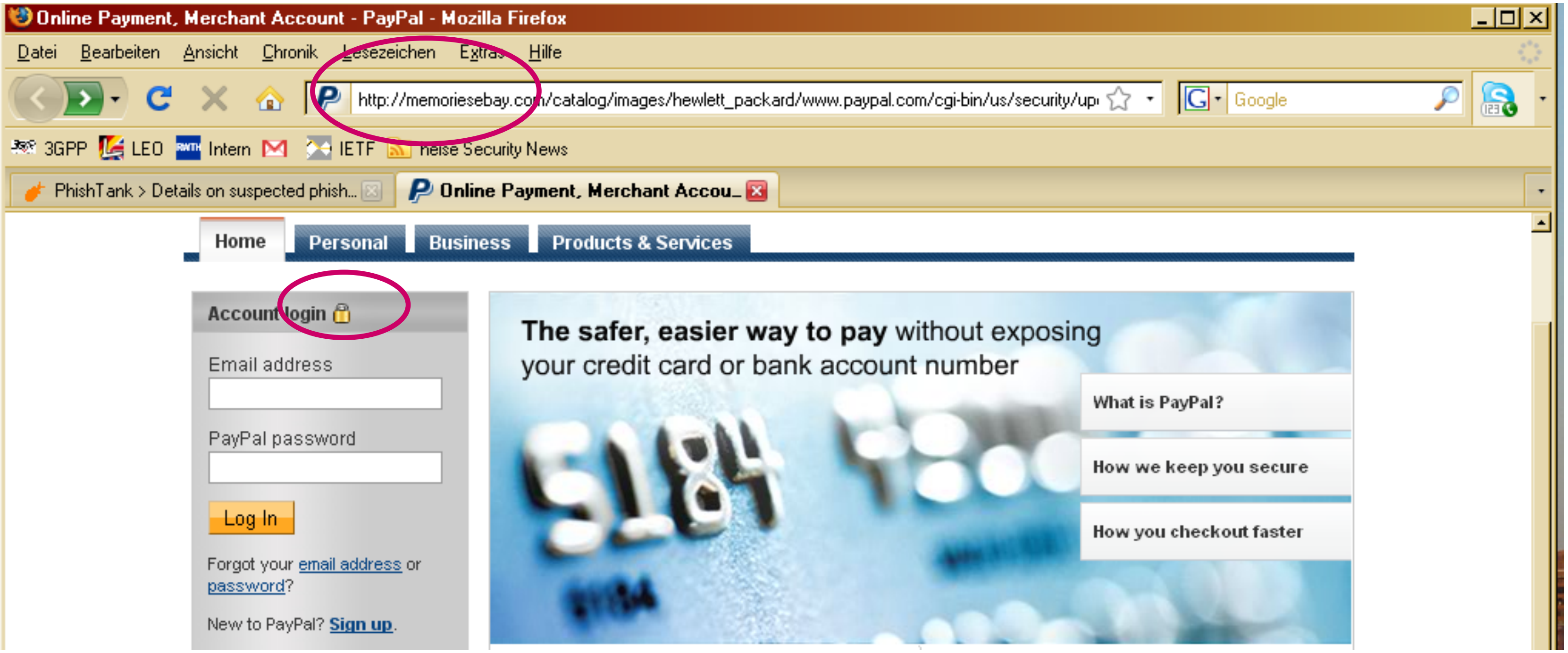
Making Fake URLs More Believable (2)

- International domain names abuse
  - International Domain Names in Applications (IDNA) enables the use of Unicode characters in the ASCII format used by the existing DNS infrastructure
  - A browser that supports IDNA interprets the ASCII representation of the Unicode characters such that the user will see the Unicode characters
  - Attackers could register domain names that contain Unicode characters that appear identical to an ASCII character in a legitimate site
    - E.g. register ebay.com with the ‘a’ being the cyrillic ‘a’
- First abuse reported in spring 2013
  - xn--paypl-uqa.com → paypàl.com
  - xn--tunes-4sa.eu → îtunes.eu
  - xn--tunes-bta.fr → ïtunes.fr

Making Fake Websites Believable

- Use one of the above to make the URL displayed believable
- Use the logos of the legitimate site
- Use the same layout
- Link to some of the legitimate sites of the brand on the fake page
- Add the pad lock somewhere to deceive (more security aware) users into believing that entering the account information is secure

Example 1 [PhishTank]



http://memoriesebay.com/catalog/images/hewlett_packard/www.paypal.com/cgi-bin/us/security/up

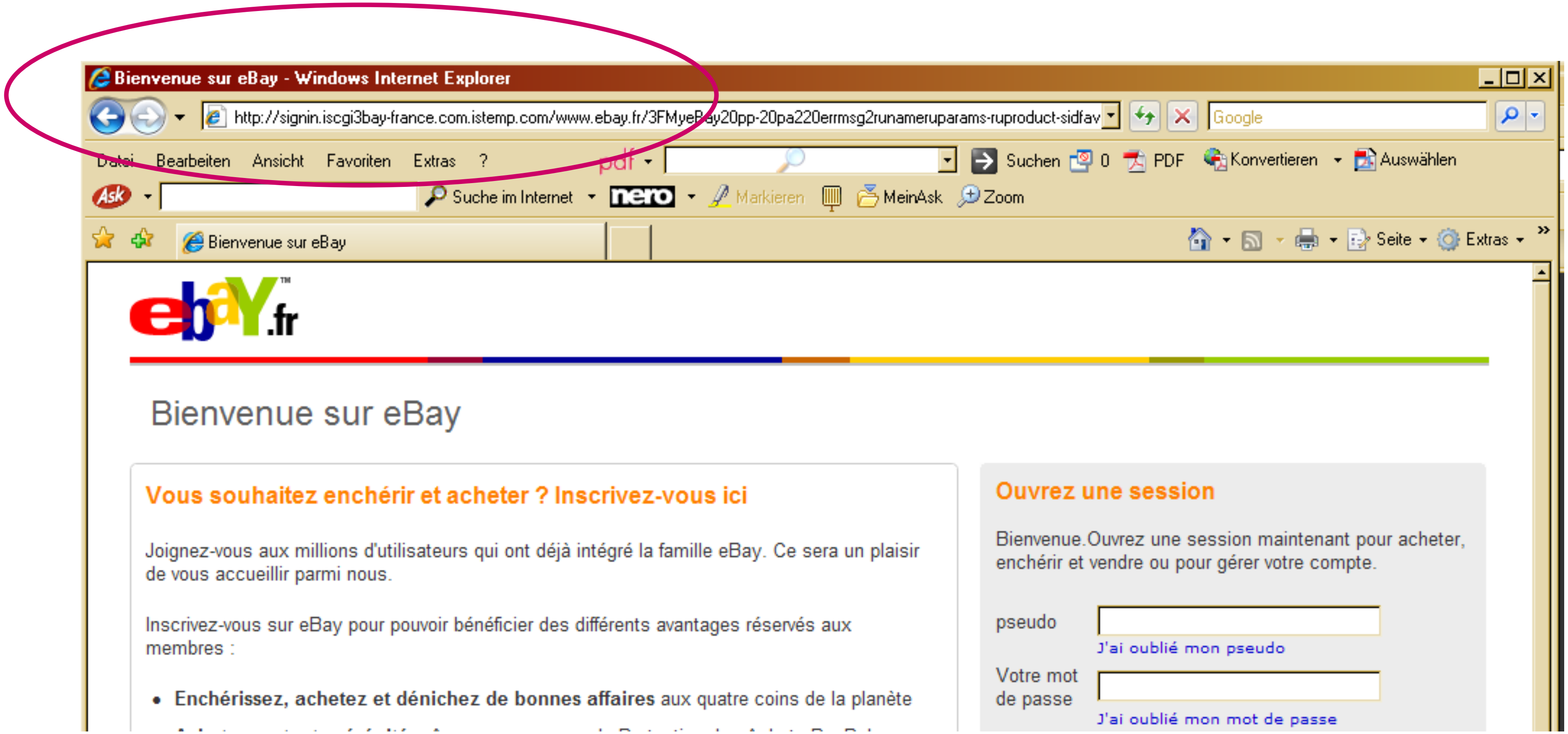
Forgot your email address or password?

New to PayPal? Sign up.

The safer, easier way to pay without exposing your credit card or bank account number

- Faked PayPal site
- No https and weird URL
- Misleading lock icon

Example 2 [PhishTank]



http://signin.iscgi3bay-france.com.istemp.com/www.ebay.fr/3FMyeBay20pp-20pa220errmsg2runameruparams-ruproduct-sidfav

Bienvenue sur eBay

Vous souhaitez enchérir et acheter ? Inscrivez-vous ici

Joignez-vous aux millions d'utilisateurs qui ont déjà intégré la famille eBay. Ce sera un plaisir de vous accueillir parmi nous.

Inscrivez-vous sur eBay pour pouvoir bénéficier des différents avantages réservés aux membres :

- **Enchérissez, achetez et dénichez de bonnes affaires** aux quatre coins de la planète

Ouvrez une session

Bienvenue.Ouvrez une session maintenant pour acheter, enchérir et vendre ou pour gérer votre compte.

pseudo

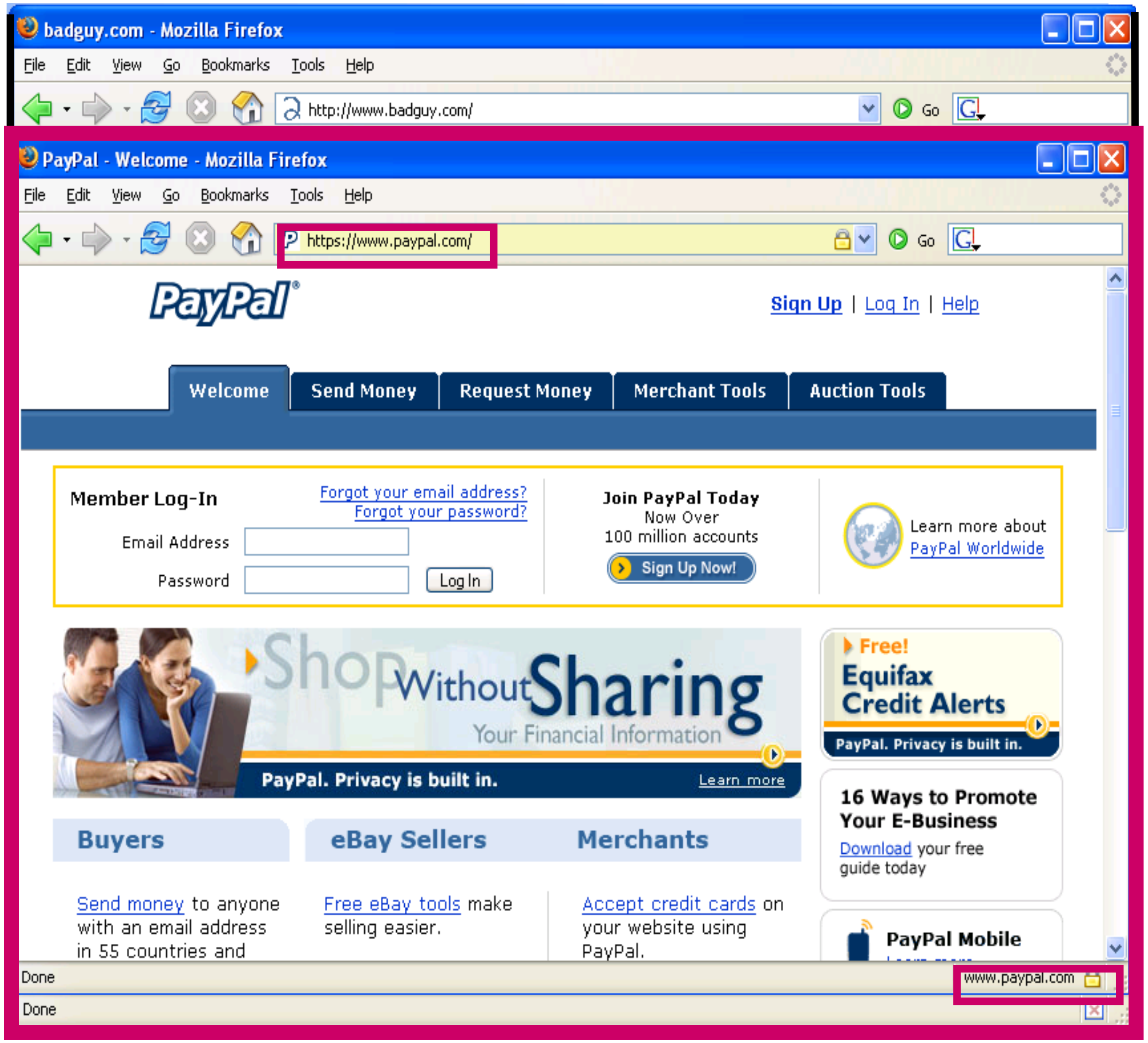
J'ai oublié mon pseudo

Votre mot de passe

J'ai oublié mon mot de passe

- Again no https, weird URL

Or Even Like This



Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Join PayPal Today
Now Over
100 million accounts

Learn more about PayPal Worldwide

PayPal. Privacy is built in. Learn more

Free! Equifax Credit Alerts

PayPal. Privacy is built in.

16 Ways to Promote Your E-Business

Download your free guide today

Send money to anyone with an email address in 55 countries and

Free eBay tools make selling easier.

Accept credit cards on your website using PayPal.

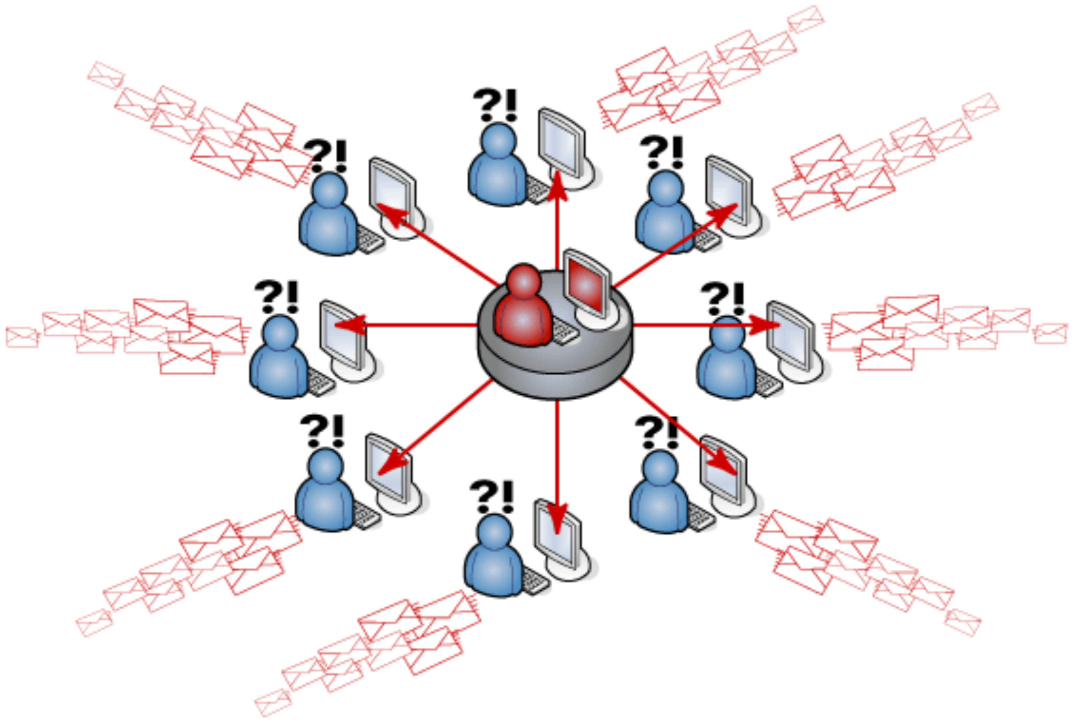
PayPal Mobile

Techniques Used to Get Faked Websites Online

- Hosting on compromised web servers
  - Attacker scans for vulnerable servers
  - Server is compromised and a rootkit or password protected backdoor installed
  - Phishers gain access to the server through this encrypted backdoor
  - Pre-built phishing websites are uploaded
  - Mass emailing tools are used to advertise the fake website
- Port redirection on compromised web servers
  - Instead of hosting the phishing websites on the compromised server, sometimes redir tool is used and configured to redirect incoming TCP traffic to a port on a remote server operated by the attacker
  - Use victim web server’s domain name in phishing emails

Spreading Phishing Email

- Same techniques as for spam
- Mostly using botnets, i.e., networks of compromised computers, that are remotely controlled by an attack



Protecting Against Phishing

- Awareness and Education
  - Helps against classical phishing
  - More awareness of connection between phishing and malicious code required
- Taking down the phishing sites
  - Average uptime of phishing sites was down to 3.1 days at most in 2010 already
  - Problem: phishers take advantage of dynamic DNS which allows a static domain name to be mapped to changing IP addresses
- Secure web browsers
- Virus, spyware and spam prevention

Web Browsers and Toolbars

- Anti-phishing tools that aim to detect phishing websites are typically implemented as browser toolbars
- Identify web pages as phishing sites by
  - Whitelists
  - Blacklists
  - Heuristics
    - Country of domain registration
    - Duration of registration
    - Popularity
  - Community ratings
    - User ratings

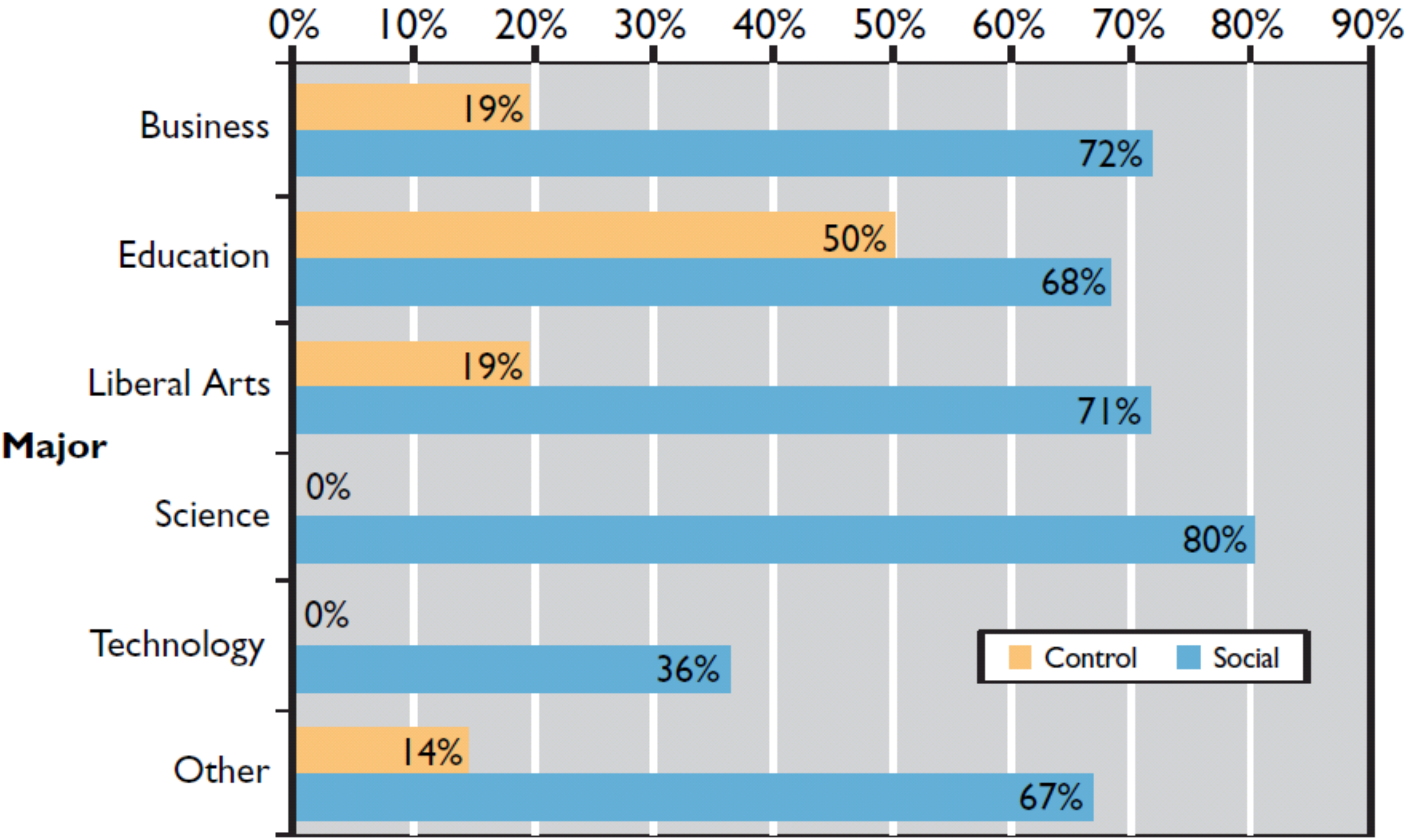
Example: Study on Spear Phishing

- Study “Social Phishing” by Jagatic et al. conducted in 2005 at Indiana University
- Used freely available information from social networks to determine strong links between students
- Students were sent a phishing email directly addressed to them
  - Sender address spoofed to be an address of one of their friends
- When clicking on the link in the phishing email
  - Students were directed to a web page
  - Web page asked them to enter their user name and password information for their university account
- A control group received the same email from an unfamiliar university email address

Results (1)

- 72% of the students fell for the attack with a friend as sender
- 16% of the students in the control group fell for the attack
- Females were more likely to fall for the attack
  - 77% vs. 65%
- Males fell for the attack more often if email was sent from female
  - 68% vs. 53%

Results per Major [Jagatic et al.]



How Serious is Phishing?

- Some quotes on how much money is in the phishing business
  - RSA 2013 Fraud Report, estimates global losses from phishing at $1.5B in 2012.
  - ‘U.S. consumers were scammed out of roughly $3.2 billion over the past year from phishing scams’ (Gartner Inc. 2007)
  - ’$15.6 billion scammed out of US adults on identity theft’
    - Federal Trade Commission 2006, does not only count phishing
  - ‘$500 million loss in the US’ (Truste 2004)
  - ‘$367 million phishing losses/year in the US’ (Javelin 2005)
- In addition it is typically assumed that the access boundary to the “phishing market” is low

Problems with the Numbers

- Take average loss reported by victim and scale that to the entire population
  - Single exaggerating reports have big impact
  - Using the median instead of the average would be better
- Very hard to randomly select online users
- Refusal rates of users to participate in surveys is very high
- Participants tend to report incidents that do not fall in the time period in question
- Other may forgetting incidents, especially if the consequences were not that bad
- …

References and Resources

- Anti-phishing Working Group
  - http://www.antiphishing.org/
- PhishTank
  - http://www.phishtank.com/stats.php
- Technical Trends in Phishing Attacks (US-CERT)
  - www.cert.org/archive/pdf/Phishing_trends.pdf
- C. Herley, D. Florencio: A Profitless Endeavor - Phishing as Tragedy of the Commons, 2008
- T. Jagatic et al.: Social Phishing, 2007
- Y. Zhang et al.: Phinding Phish - Evaluating Anti-Phishing Tools, 2007
- S. Egelman et al.: You've been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings, 2008
- S. Sheng et al.: Who Falls for Phish? A demographic Analysis of Phishing Susceptibility …, 2010