



Social Phishing

Tom Jagatic
Nate Johnson
Markus Jakobsson
Filippo Menczer

Dept. of Computer Science
School of Informatics
Indiana University, Bloomington

<http://www.indiana.edu/~phishing/>

free newsletters

Sign up today!

Site Search

enter here

go

[Go to other searches](#)

Free Newsletters

[The Connection](#)[Books & Culture](#)[Building Church Leaders](#)[ChristianBibleStudies.com](#)[Christian History](#)[Christian Sports](#)[Connection](#)[Church Leaders](#)[CTDirect](#)[Marriage](#)[Music](#)[Parenting](#)[Preaching Today](#)[PT Sermons & PT Audio](#)[Singles](#)[Small Groups](#)[Teens](#)[Women](#)[Your Spiritual Life](#)

Risk-free Magazine

Subscriptions

[Christianity Today](#)[Books & Culture](#)[Campus Life](#)[Christian History](#)[Christian Parenting](#)[Today](#)[Christian Reader](#)[Leadership Journal](#)[Marriage Partnership](#)[Men of Integrity](#)[Today's Christian](#)[Woman](#)

All e-mail newsletters from ChristianityToday.com will have the following in the From line:

@lists.christianitytoday.com

Examples:

The HTML version of the Connection newsletter says

From: Connection-HTML@lists.christianitytoday.com

The plain text version of the Women's Connection says

From: Women@lists.christianitytoday.com

**The Connection**

Delivered via e-mail each week, this newsletter's purpose is to keep you informed of what's happening in our dynamic online community.

Subscribe now

enter your e-mail

go

[View past issues here](#)**Books & Culture**

Each weekly issue contains up-to-date, insightful information about today's culture, plus analysis of books important to the evangelical thinker.

Subscribe now

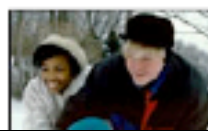
your e-mail

go

[View sample newsletter here](#)**Building Church Leaders**Each bi-weekly issue contains new articles and insights on leadership training, updates on what's been added to [BuildingChurchLeaders.com](#), and other practical help to build faithful and effective leaders in your church.**Subscribe now**

your e-mail

go

[View sample newsletter here](#)**Campus Life Connection**

Hot music! Lots of laughs. Relationship advice. True stories on life and faith ... all this and more in our weekly teen newsletter.

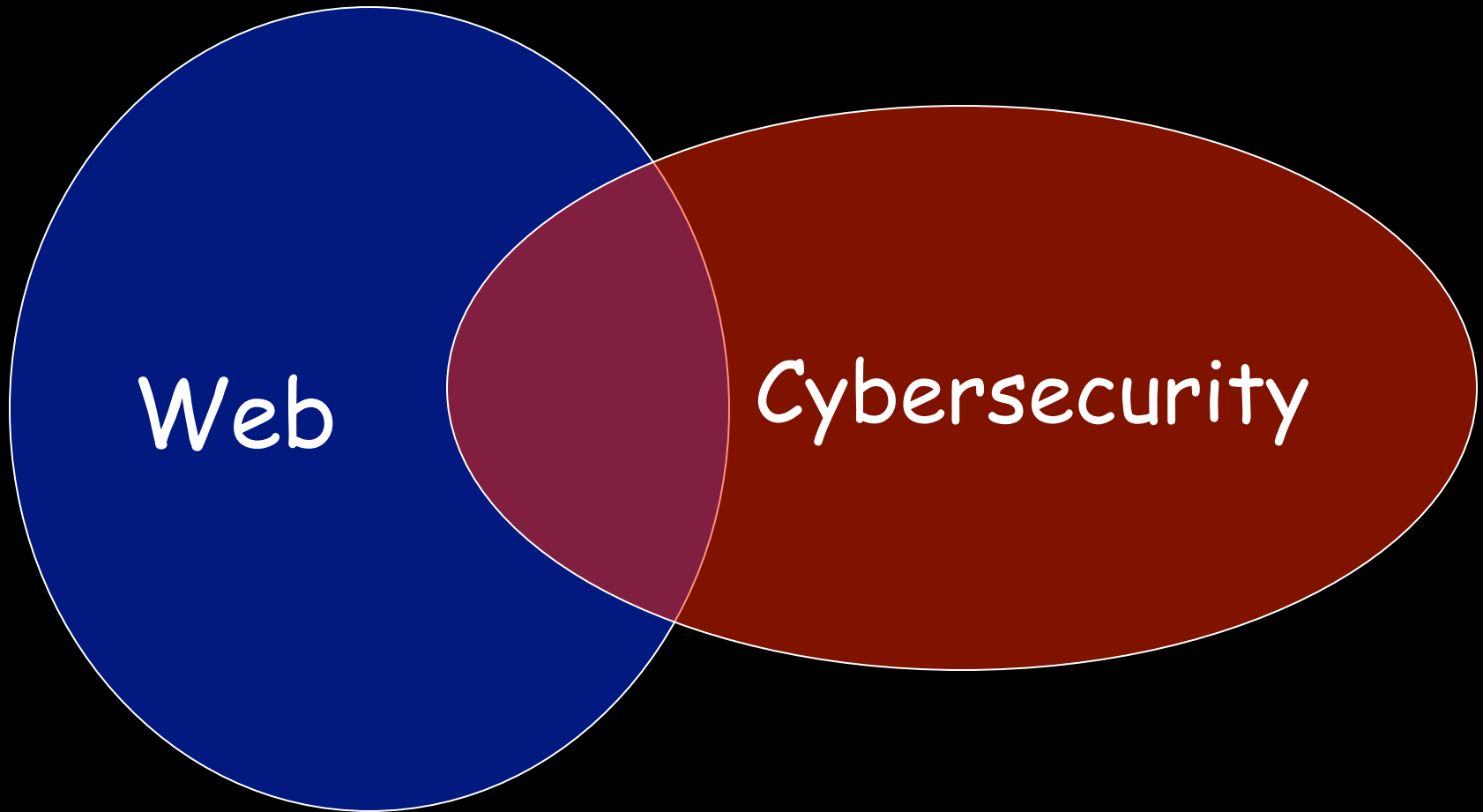
Subscribe now

enter your e-mail

go



Motivation



Phishing for Clues

Inferring Context Using Cascading Style Sheets and Browser History

[Markus Jakobsson](#), Tom N. Jagatic, and [Sid Stamm](#)

[Read/Post Comments -- Browser Recon Weblog](#)

The strongest indication consumers get that a particular phishing email is not legit is that it is "sent by" an institution they do not have any relation with. For example, a person who banks with CitiBank and AmeriTrade is not going to believe an email appearing to be sent by Chase or etrade, asking him or her to confirm his password. To improve the yield, phishers are likely to try to automatically extract as much information they can about their victims, then target them in manners that are consistent with the context. More concretely, if a phisher could determine banking relationships, he would not have to spoof the "wrong" entities when targeting victims. Alarmingly, this is rather straightforward to do, and hard to protect against.

One can use a simple technique used to [examine the web browser history](#) of an unsuspecting web site visitor using Cascading Style Sheets. This technique is particularly worrisome in the problem domain of phishing. Phishers typically send massive amounts of bulk email hoping their lure will be successful. Given greater context, such lures can be more effectively tailored---perhaps even in a [context aware phishing attack](#). It should be emphasized the following attack can be launched from any arbitrary web site and is embedded in HTML markup. Many web browsers are susceptible.

An illustrative example

If I were a phisher, I would be glad to know you bank with:

[\[click to learn more \]](#)



Demonstration: [View](#) all "sites of interest" within your own browser history.

Send a browser-recon.info link to a friend

Your Name:

Your Email:

Friend's Name:

Friend's Email:

Would you like to know if your friend has visited any "sites of interest?" ☒ yes ☐ no

Note: Only your name will be shared with the recipient of the message. Notification messages of friend browser history will only indicate if this technique was successful.

Phroogle™ Order

Phroogle™ -- Too Good To Be True

As you surely figured out, this was a demonstration of a [phishing](#) attack. In this new, dangerous type of phishing, the attacker guesses an attractive low price using a comparison shopping site such as Froogle or Yahoo Shopping.

The phisher can also attract victims to a fake site like this by publishing artificial prices through comparison shopping sites such as Froogle or Yahoo Shopping.



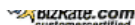
You visited this site before, therefore we did not count this visit toward our statistics.

Here are some statistics about visitors:

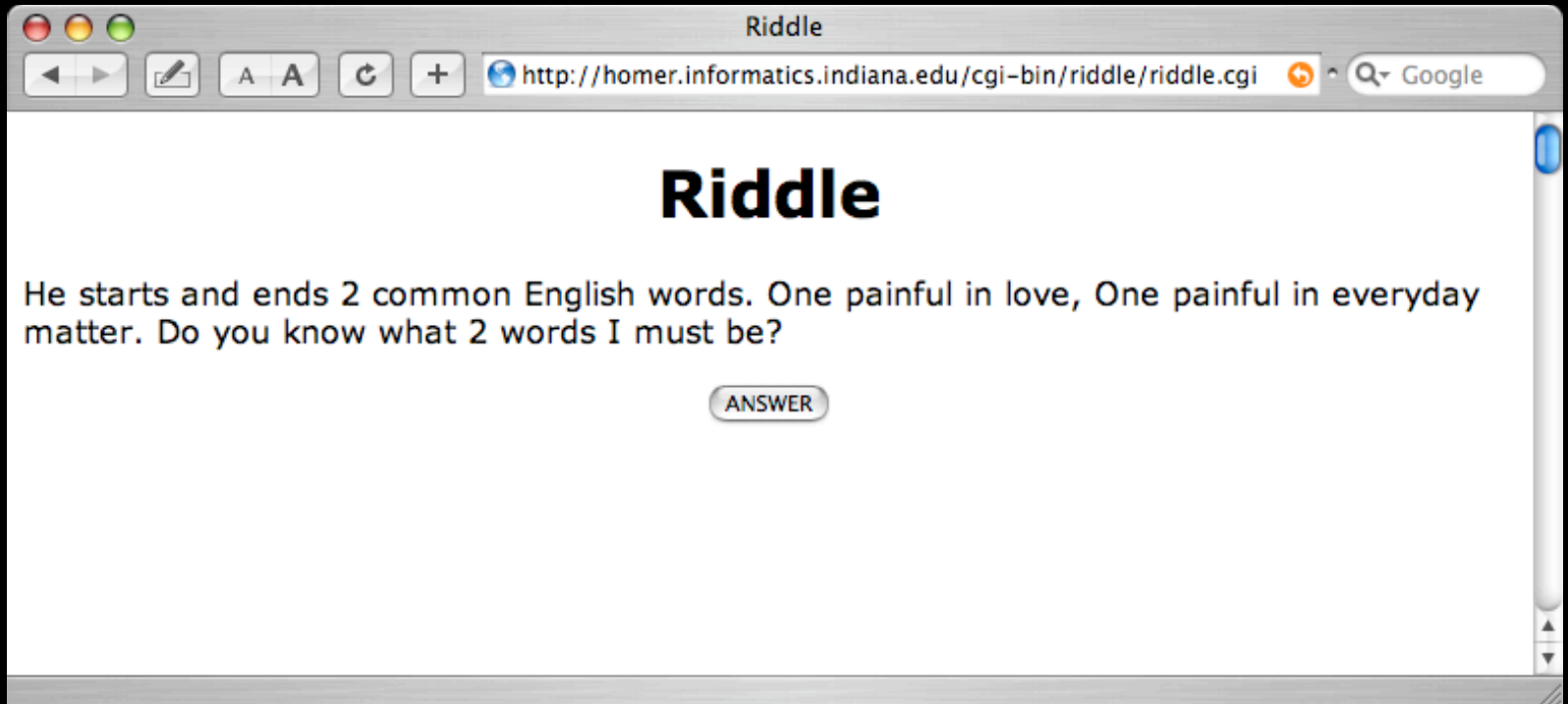
Number of people who visited the site (total)	28 (100 %)
Number of people who visited the site (unique)	17 (60 %)
Number of people who submitted queries (unique)	16 (57 %)
Number of people who proceeded to order (unique)	8 (28 %)
Number of people who entered credit card information (unique)	1 (3 %)
Number of people who entered bank account information (unique)	2 (7 %)



© 2005 [Filippo Menczer](#) @ [Phishing Research Group](#)



© 2005 [Filippo Menczer](#) @ [Phishing Research Group](#)



www.indiana.edu/~phishing



Outline

- **Social phishing** = id-theft attack exploiting social network context
- How to harvest social networks from the Web
- An experiment
- Results
- Discussion: why, how, reactions, ethics



Questions

Web Mining:

How easy is it to mine actionable information about people's *social networks* from public Web sites?

**social
phishing**

Cybersecurity:

Can phishing attacks become more effective (dangerous) by exploiting *context* information about targets (victims)?



Larry's network

[Larry Page](#)

male

Mountain View, CA

Interested in:

friends, activity
partners, business
networking[view profile](#)[view friends](#)[Andrew](#)
(179)[Ben](#) (144)[Brad](#) (359)[Meredith](#)
(66)[Frederique](#)
(88)[Marcel](#) (151)[Chade-Meng](#)
(221)[Naga
Sridhar](#) (38)[Jeff](#) (206)[Orkut](#) (567)[Amit](#) (334)[Rob](#) (158)[Niniane](#)
(170)[Sara](#) (208)[David](#) (88)[David](#) (279)[Bojan](#) (66)[Valentin](#)
(477)[David](#) (307)[Adrian](#) (43)[Bret](#) (85)[Brett](#) (100)[Dzevad](#)
(177)[Dennis](#)
(128)[Lauren](#) (53)[Nina](#) (93)[Clara](#) (320)[Steve](#)
(1054)[Walma](#) (47)[Lydia](#) (97)[Sanford](#)
(182)[Wei-Hwa](#)
(287)[Leslie](#) (114)[Gil](#) (105)[Georges](#)
(114)



Welcome, Filippo



[Sign Out](#)

[Your Account](#)

[+ Add Connections](#)

[Home](#)

[Find People](#)

[Find Jobs](#)

NEW!

[Find Services](#)

[My Profile](#)

[My Contacts](#)

[Connections](#)

[Sent Invitations](#)

[Other Contacts](#)

[Colleagues](#)

[Received Invitations](#)

[Settings](#)



Browse Markus Jakobsson's Connections



[Go Back to Connections](#)

Markus Jakobsson

Associate Prof & Associate Director at IUB

Bloomington, Indiana Area

Currently: Associate Prof & Associate Director at IUB

Companies: IUB

Primary Industry: Computer & Network Security

Connections / Network



6

Markus's Connections: 6
You and Markus are **connected**.

Markus's Connections

[Filippo Menczer](#)

Associate Professor of Informatics and Computer Science, Indiana University

[Adam Young](#)

Research Scientist at Cigital Inc.

[Virgil Griffith](#)

Research Assistant at Indiana University and Student at Indiana University

[Shouhual Xu](#)

Professor at University of Texas, San Antonio

[Hampus Jakobsson](#)

Marketing Manager at TAT AB and Owner, TAT AB (TAT works with UIs for contained systems)

[Hein R](#)

Computer Scientist and Software Engineer

[Go Back to Connections](#)



[thefacebook]

[home](#) [search](#) [global](#) [social net](#) [invite](#) [faq](#) [logout](#)

Virgil Griffith !'s Profile

Indiana

quick search go[My Profile \[edit \]](#)
[My Friends](#)
[My Groups](#)
[My Parties](#)
[My Messages](#)
[My Account](#)
[My Privacy](#)**BUSTED TEES**
FUNNIEST. TSHIRTS.
ANYWHERE.

Picture

[Send Virgil a Message](#)[Poke Him!](#)[Add Virgil as a Friend](#)

Access

Virgil last logged in from a non-residential location.

Friends at Indiana



Kim Hedge

Marisa
GeogheganRebecca
McOright

Eric Nichols



Jordan DeLong

Michael
AmlungVirgil has 30 friends at Indiana.
[see all of them]

Other Schools

Information

Account Info:

Name: Virgil Griffith ! [add to friends]
Member Since: September 28, 2004
Last Update: May 17, 2005

Basic Info:

School: Indiana '06
Status: Student
Sex: Male
Concentration: Cognitive Science
Computer Science
Birthday: 03/06/
High School: Alabama School Of Math And Science '02

Contact Info:

Contact Email: virgil@yak.net
School Email: griffitd@indiana.edu
Screenname: Romanpo3t
Websites: <http://www.romanpoet.org>
<http://www.romanpoet.org/141>

Personal Info:

Interests: Analytic Philosophy, Puffins, German, SCIENCE!, technology, Mind, Chemistry, Computer Security, Consciousness, Bunnies
Clubs and Jobs: Security H4x0r for Informatics.
Favorite Music: REM, Kraftwerk -- Noise, Ambient. Things mostly very grating on the ears.
Favorite Books: GEB, Ted Nelson's 'Literary Machines'
Favorite Movies: Clockwork Orange, Battle Royale, I generally like dark films.
Favorite Quote: We must know, We will know.
-- David Hilbert's tombstone
About Me: If I were guaranteed success in only one thing in life, I would solve consciousness.*****
In some circles I am known for my work on a campus card system that is likely in use at your university.

Summer Plans

Job/Activity: Santa Fe Institute REU
Location: Santa Fe, NM, Pasadena, CA, Caltech, 87501
Additional Info: <http://www.santafe.edu/education/reu/200...>Will also be around Pasadena for:
<http://assc.caltech.edu/index.htm>



simsong - User Info

 **LiVE JOURNAL™**

Not logged in.
([Create account.](#))

WelcomeSearchHelpAbout

LoginCreate an AccountUpdate Your JournalEnglishEspañolDeutschРусский→

Search: Category: Username

User Info

User Information

Below is user information for Simson Garfinkel. If you are this user, you can edit your information (or choose what information is considered public) at [the Edit Info page](#).



User: [simsong](#) (850164) 

Name: Simson Garfinkel

Website: [Simson's Home Page](#)





Location: [Belmont](#), [Massachusetts](#), [United States](#)

Birthdate: 1965-07-12

E-mail: simsong@acm.org

Bio: Simson Garfinkel is a graduate student at MIT.

Interests: 4: [cryptography](#), [journalism](#), [law](#), [programming](#). [[Modify yours](#)]

Friends:  1: [bjaspan](#)
 4: [csci_e_170](#), [csci_e_170a](#), [lj_clients](#), [lj_dev](#)
 5: [ms_secbulletin](#), [msft_briani](#), [simson_net](#), [techreview](#), [techreview_blog](#)

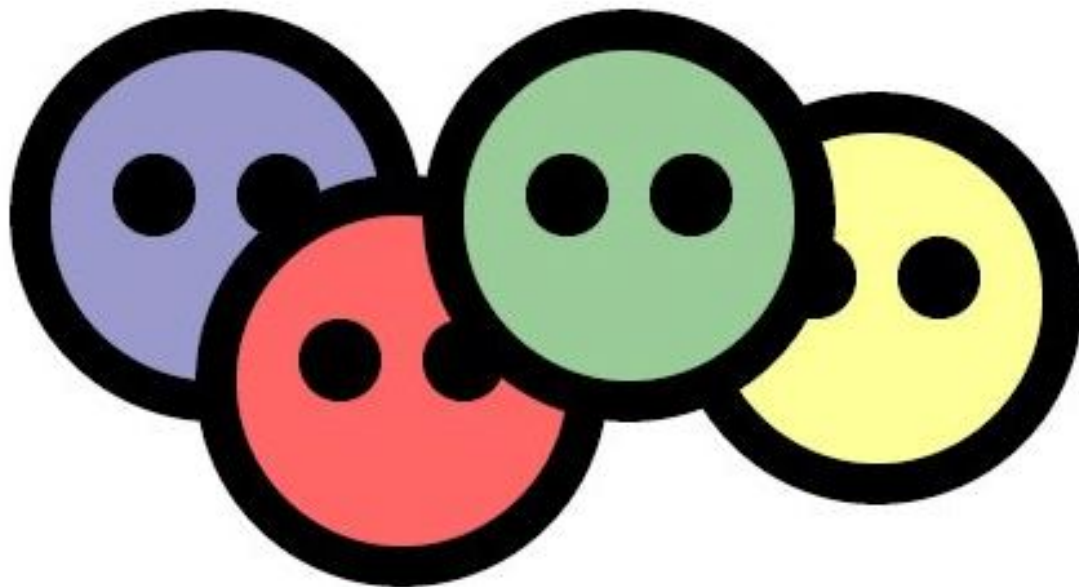
Friend of: 14: [agaran](#), [anaisdjuna](#), [anotherjen](#), [catya](#), [chanaleh](#), [drglam](#), [erikjn](#), [ivorjawa](#), [kill](#), [marypcb](#), [mr_privacy](#), [silentbamboo](#), [src](#), [xthread](#)

Member of: 4: [csci_e_170](#), [csci_e_170a](#), [lj_dev](#), [paidmembers](#)



the foaf project

The *Friend of a Friend* (FOAF) project is about creating a Web of machine-readable homepages describing people, the links between them and the things they create and do.



Associate Research Professor
[Computer Science](#) and
[Engineering & Public Policy](#)

[Carnegie Mellon University](#)
5000 Forbes Avenue
Pittsburgh, PA 15213

office: CIC 2207
phone: 412-268-7534
email: lorrie AT cs DOT cmu DOT edu

Executive Assistant:
Jennifer M. Lucas
phone: (412) 268-9870
email: jmlucas AT cs DOT cmu DOT edu



My current research focuses mostly on online privacy. I am particularly interested in applications of the Platform for Privacy Preferences ([P3P](#)), and in user interfaces and usability issues related to privacy enhancing software and [secure systems](#). I chaired the P3P Specification working group and designed the [AT&T Privacy Bird](#) P3P user agent. I completed a [book on P3P](#) in 2002. Other recent work includes a study on [security vulnerabilities in the movie production and distribution process](#). I have also done research on [electronic voting](#) and a novel voting procedure called [declared-strategy voting](#).

I came to [Carnegie Mellon University](#) in December 2003 after seven years at [AT&T Labs-Research](#). I am a faculty member in the [Institute for Software Research, International](#) in the [School of Computer Science](#) and in the [Engineering and Public Policy](#) department in the [College of Engineering](#). I am director of the [CMU Usable Privacy and Security Laboratory \(CUPS\)](#). I am also affiliated with the [Ph.D. Program in Computation, Organizations and Society](#), [Cylab](#), the [Human-Computer Interaction Institute](#), and the [Privacy Technology Center](#).

I spend most of my free time with my husband ([Chuck](#)), son ([Shane](#)), and daughter, ([Maya](#)). Sometimes I find time to design and create [quilts](#).

Chuck Cranor's Web Page Index

Contact information:

email:

username: chuck
host: netbsd.org

Chuck's pages:

- [Carnegie Mellon University page](#) [this is where I currently work]
- [NetBSD page](#)
- [University of Delaware page](#)

Old pages (no longer available -- don't bother looking for them):

- Washington University page
- AT&T Research page

Related pages:

- [Lorrie Faith Cranor \(my wife\) page](#)
- [Shane Zachary Cranor \(my son\) page](#)
- [Maya Quinn Cranor \(my daughter\) page](#)

Chuck Cranor, May 2005.

Shane Zachary Cranor



[Photo Album](#) | [Latest Photos](#) | [2001 Favorite Photos](#) | [2002 Favorite Photos](#) | [2003 Favorite Photos](#)

Watch a movie of Shane at 2 1/4 putting on his sandals and talking about mowing the lawn. "What am I doing?" he asks. "I'm putting them on slowly," he says (he really means "loosely"). If you are not sure what he's saying, [read the transcript](#).

Shane's Photo Album

- [Shane's First Year](#)
- [Shane's Second Year](#)
- [Shane at 24-25 Months](#)

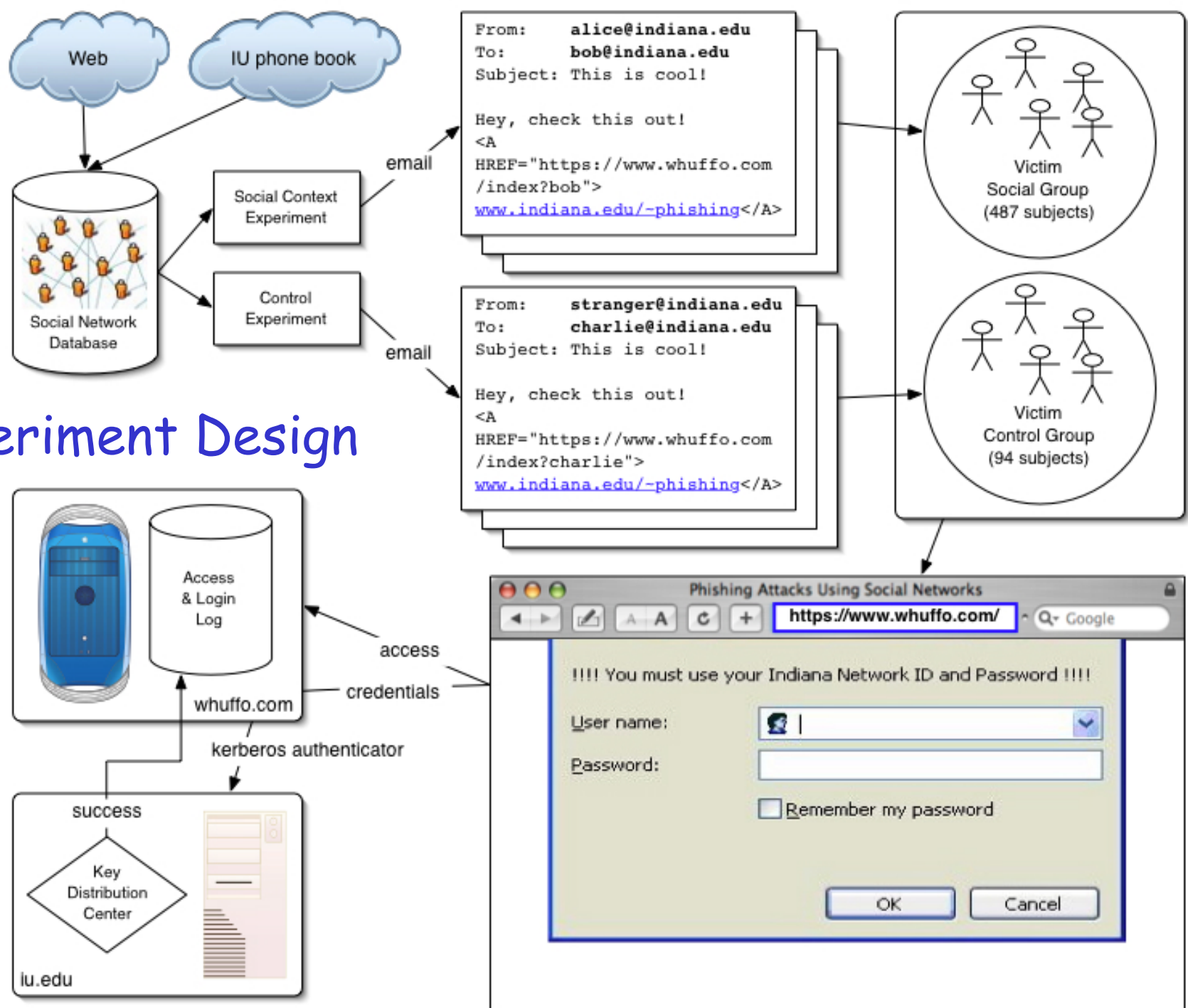
Maya Quinn Cranor



Born Friday, September 19, 2003, 5:15 pm
7 pounds, 13 oz., 21 inches

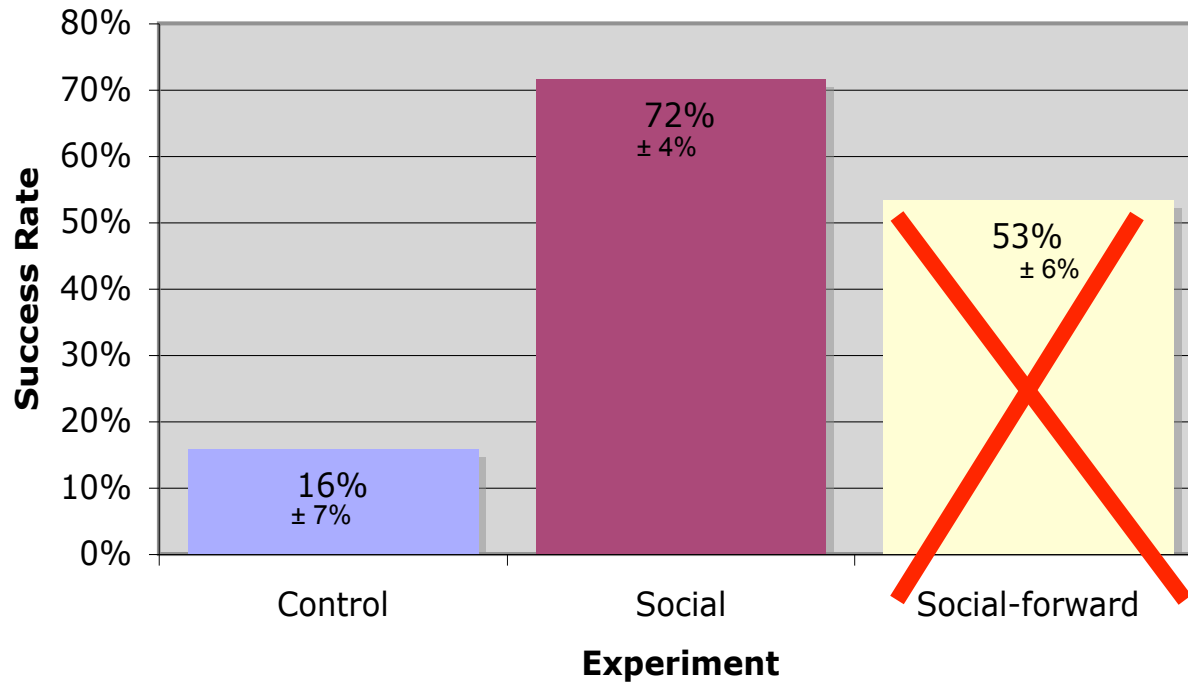
Maya's Photo Album

- [2003 Favorite Photos](#)
- [2004 Favorite Photos](#)





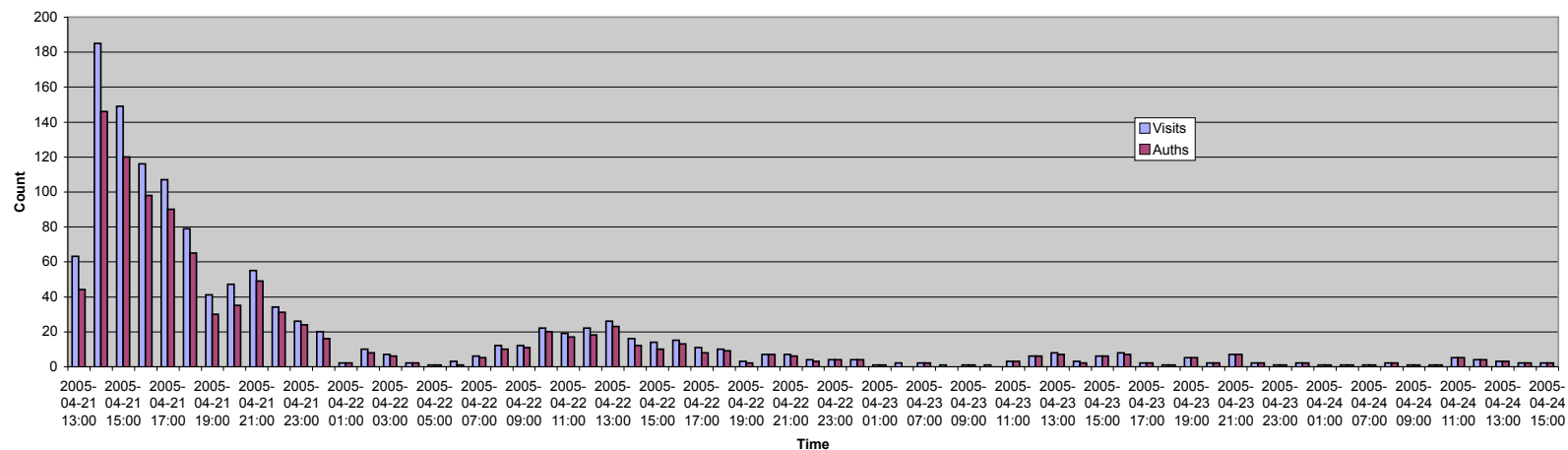
Main Result



$$p < 10^{-6}$$

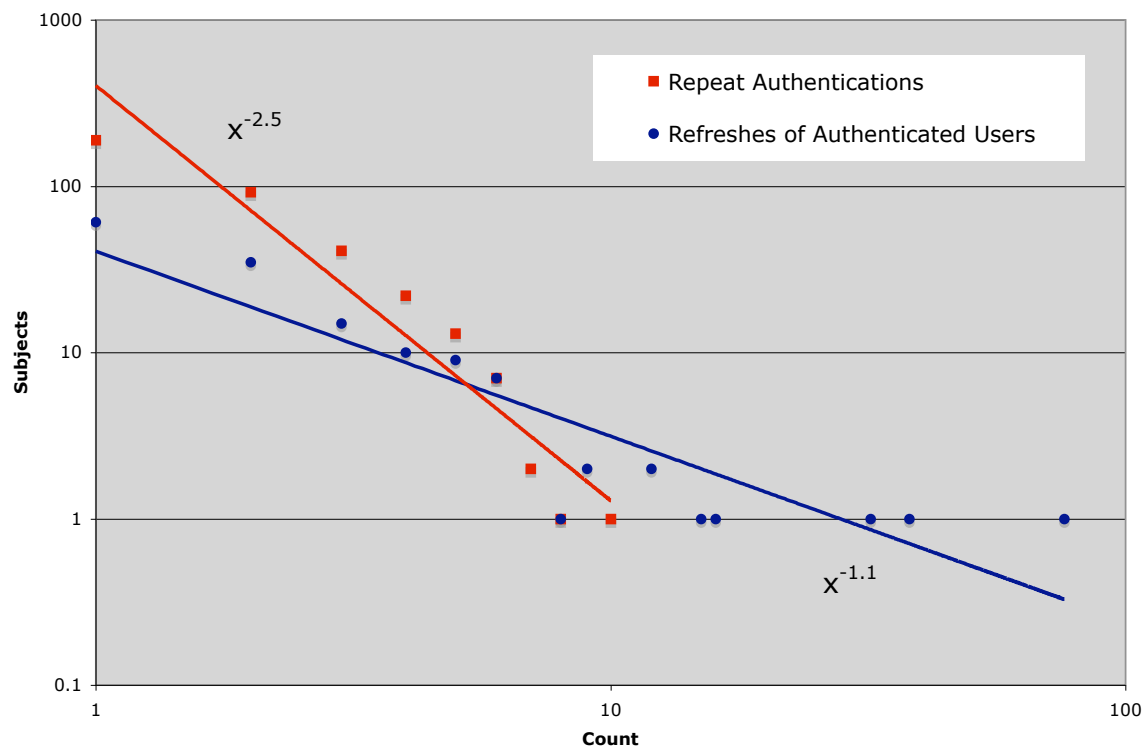


Unique Visits and Authentications per Hour



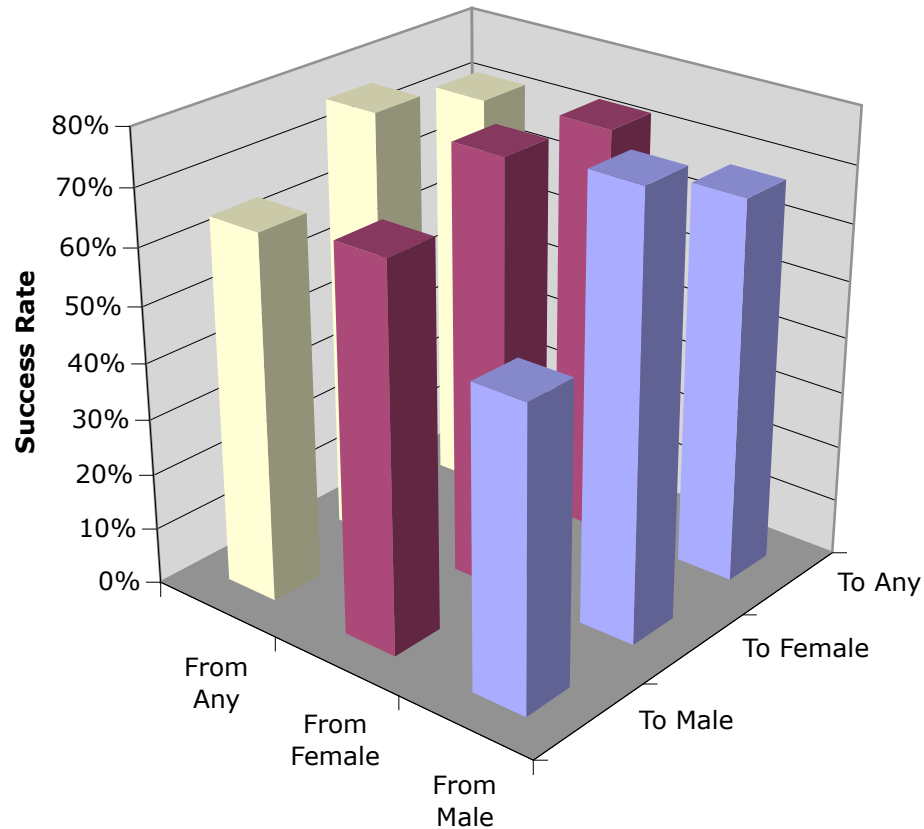
Response Dynamics

Repeat Hits





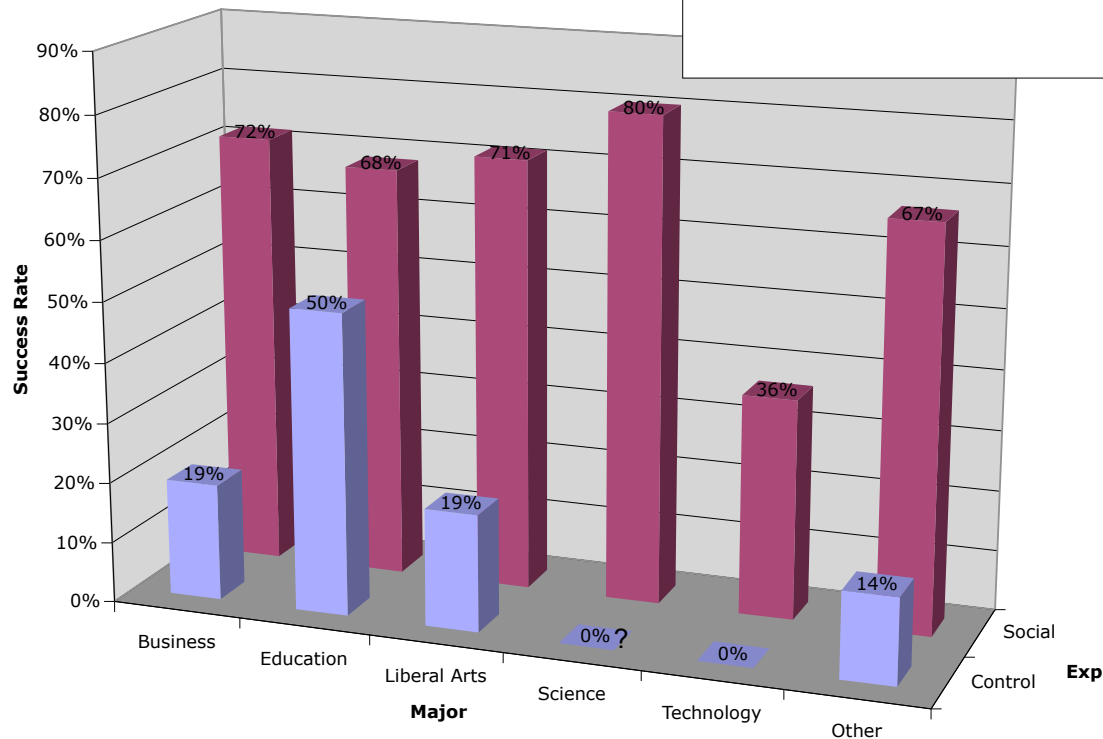
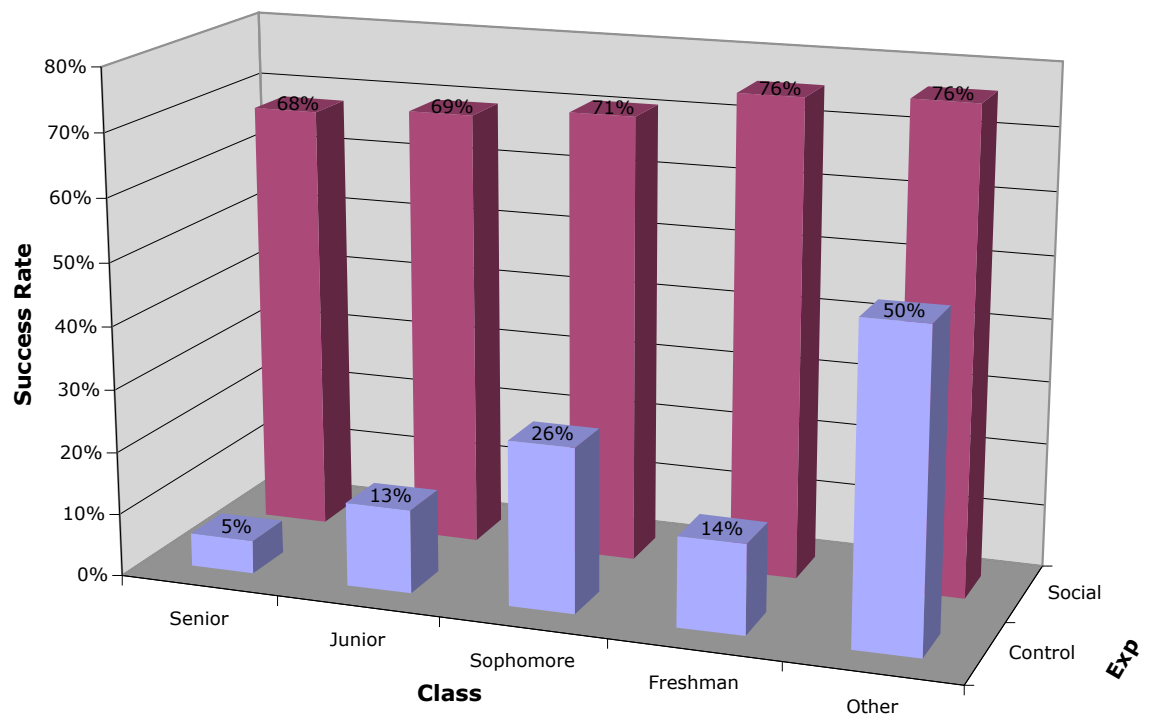
Gender Effects



	To Male	To Female	To Any
From Male	53%	78%	68%
From Female	68%	76%	73%
From Any	65%	77%	72%

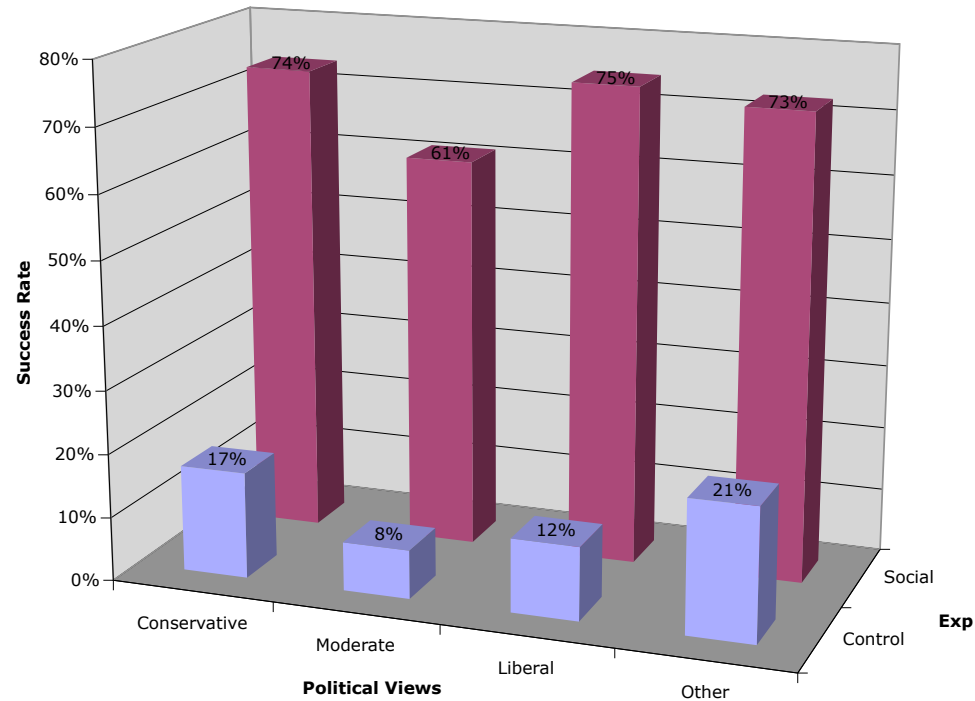


More Demographics





More Demographics





Human Subjects Approval

- **Two parts:**
 1. Collection of social network data, IU 18-24 (exempt)
 2. Phishing attack experiment (IRB full review)
- **Benefits:**
 1. determine actual number of people (college-aged/college students) who would respond to a phishing attack by providing personal information
 - objective baseline essential for development of countermeasures (defenses) to reduce vulnerability via computer software and educational programs
 2. assess the influence of social context (being attacked via a friend's spoofed email address or via an unknown address)
 3. assess how easy it is to use publicly available information to stage a phishing attack
 4. increase awareness in the general public about phishing and the dangers of disclosing personal information on the Web



Human Subjects Approval

- **Waiver of Consent (CFR 46.116(d))**
 1. no more than minimal risk
 2. not adversely affect rights and welfare of subjects
 3. research could not practicably be carried out without waiver
 4. pertinent information after participation
 - Debriefing email, information web site, anonymous blog
- **Deception**
 - “only when there are no viable alternative procedures”
 - “rare instances in which no consent can be obtained [...]: e.g., if the researcher pretended to lie unconscious on a sidewalk and noted how many and what sorts of persons stopped, attempted assistance, or simply hurried past”



Reactions Timeline

4/24/2005

- End exp
- Debrief email w/links to site & blog

4/26 IDS 1st page

INDIANA DAILY STUDENT
idsnews.com

NEWS | OPINION | SPORTS | ARTS | FEATURES |
CAMPUS | CITY & STATE | NATION & WORLD

Updated: Tuesday, April 26, 2005

Students go 'phishing' for user info
Research technique used to show ease of login, username theft
By Colleen Corley | Indiana Daily Student | Tuesday, April 26, 2005

For students duped by a bogus e-mail claiming to be from the IU server, two students at the School of Informatics have a message: You've been spoofed by fictitious identity hackers.

The hackers, graduate students Tom Jagatic and Nate Johnson, conducted an e-mail experiment last week that has outraged some students and raised important questions about privacy and the public sphere. Using information gleaned from publicly available sites on the Internet, Jagatic and Johnson sent e-mails to students seemingly from e-mail addresses familiar to the students. For example, Bob@indiana.edu would receive an e-mail from his girlfriend Alice@indiana.edu. The subject would boast, "This is cool!" and the e-mail would be signed, "Alice."

"We feel very bad that the students feel violated. That doesn't mean that it was unethical or illegal."

Filipo Menczer, Informatics and computer science associate professor

The body of the e-mail instructed, "Hey, check this out!" and provided a link on the IU server that prompted students to provide their username and password. The e-mails were not actually sent from the e-mail accounts they seemed to originate from.

"It was deceptive, (but) there was no other way to conduct the study," said Filipo Menczer, an associate professor of Informatics and computer science. The study was conducted by Jagatic and Johnson as part of Menczer's graduate-level Web mining course offered through the School of Informatics. Associate Professor of Informatics Markus Jakobsson was the faculty adviser for the study.

CLASSIFIEDS
DINING SCENE
HEALTH DIRECTORY
HOUSING GUIDE
RELIGIOUS DIRECTORY
HAPPENINGS CALENDAR
ADVERTISING
ABOUT THE IDS

ELECTRONIC EDITION

The college

4/27
Blog closed
(440 posts)

4/27
UITS
news,
KB
updated

4/28 IDS 1st page

INDIANA DAILY STUDENT

ENGLISH CASE
BASIC V BACK
WHEELS
56
48

securing
cyberspace

Symposium tackles university cybersecurity issues, shortcomings
By Kathleen Quilligan
Informatics Daily Student

When I first heard about this I was like, you've got to be kidding... but you can't do this type of research and tell people in advance.

'Phishing' experiment attracts national adulate about ethics of study
By Colleen Corley
Informatics Daily Student

After students discovered that graduate students Tom Jagatic and Johnson were behind a spoofed identity theft attack sent out through e-mail last week, students expressed their anger and surprise by writing more than 200 comments on the matter of Internet ethics and privacy. The spoof attack was part of a study of identity theft, "phishing," sponsored by a Web mining course in the Computer Science Department. The experiment aimed to test people's reactions to being "phished" by acquaintances or friends, whose e-mail account would send a message including a link that prompted students to provide their IU usernames and passwords. Jagatic and Johnson, both graduate students in the Computer Science department, obtained

see SYMPOSIUM, page 10
see PHISHING, page 10

4/21
Start
exp

4/25
65
posts
on blog

Slashdot
It is what IT is.

Phishing for Credit
Posted by Zonk on Tue Apr 26, '05 04:55 PM from the both-academic-and-financial dept.
An anonymous reader writes "Two graduate students at Indiana University conducted a phishing study to determine how readily students will give up personal information if the phishing emails appear to come from close friends. Using only publicly available information, they sent out emails to students asking them to click a link that required username/password information. Needless to say, the study has generated lots of attention on campus. The student newspaper has the story and the researchers have created a blog where the participants can vent."

Phishing for Credit | Log in/Create an Account | Top | 218 comments

4/26 (p.m.)

4/26
327
posts
on blog

4/27 IDS Editorial

INDIANA DAILY STUDENT
idsnews.com

NEWS | OPINION | SPORTS | ARTS | FEATURES |
EDITORIALS | COLUMNS

Updated: Wednesday, April 27, 2005

Staff Editorial
Students make easy bait
Research on phishing angers some unwitting subjects
By IDS Editorial Board | Indiana Daily Student | Wednesday, April 27, 2005

Thanks to your own insatiable thirst to be virtually connected, your personal information and history is widely available online, legally and illegally, to whoever wants to get it.

Two graduate Informatics students just used public Web sites (anyone?) to help them set up an experiment that tests how social connections affect responses to requests for information on the Internet.

While the research is of a vital economic and security nature, the IU campus has an interest in having students and others supporting studies at their research institution, and that support is undermined when students feel victimized. Students became human subjects without any warning.

Sure, the deception was necessary to make the experiment valid. If the selected students were warned beforehand that they would be tested on their responses to a given e-mail, the data would have been worthless.

OUR VIEW
Informatics study was legitimate, but students should have been asked before being e-mailed.

CLASSIFIEDS
DINING SCENE
HEALTH DIRECTORY
HOUSING GUIDE
RELIGIOUS DIRECTORY
HAPPENINGS CALENDAR
ADVERTISING
ABOUT THE IDS

ELECTRONIC EDITION

In May...

Hackers with hearts of gold

Cybersecurity researchers think like "the bad guys" as they tackle security problems



RESEARCH at
INDIANA
UNIVERSITY



Complaints

- 30 complaints (1.73 % of total participants) were made to the Support Center; forwarded to researchers
- Feedback to researchers:
 - Upset/complaints: 28 messages (1.6%)
 - Wanted exclusion: 7 messages (0.4%)
 - Positive feedback: 13+ messages (0.75%)
 - Majority of comments on blog and “/.” positive



Some observations gleaned from posted responses/criticisms

- **Anger:**
 - *“This was unethical/inappropriate/illegal/unprofessional/fraudolent/self-serving/useless... You should be fired/prosecuted/expelled/stomped...”*
- **Denial of one's vulnerability to phishing:**
 - *“I did not fall for it, but my friend did... I would never fall for a phishing attack...”*
- **Misunderstanding of spoofing:**
 - *“You hacked into my email account!”*
- **Overestimation of security of email:**
 - *“I can't believe IU/UITs was an accomplice!”*
- **Appreciation of email vulnerability:**
 - *“I thought I had a virus...”*
- **Underestimation of dangers of publicly posted personal info:**
 - *“How did you get my address book?... Violation of privacy... Information on [www...com] is not public...”*
- **Misunderstanding of experiment:**
 - *“Should have asked for my permission before attack”*



Other criticism of experiment

- Undue stress at end of semester
- Anonymous blog open to abuses and offensive comments
 - from subjects to researchers
 - from “/.” crowd to subjects who complained
- Exploitation of most vulnerable population (students) for benefit of wider community
- Identity deception may be illegal
- Waiver of consent should not have been granted b/c subjects' right to be treated ethically was violated
- Too many subjects? Biased sample?



How many
subjects?

$$C.I. = \frac{X}{n} \pm z_{C.I.} S_{\frac{X}{n}}$$

$$E = z_{C.I.} S_{\frac{X}{n}} = z_{C.I.} \sqrt{\frac{X}{n} \left(1 - \frac{X}{n}\right)} / \sqrt{n}$$

$$n = \left(\frac{z_{C.I.}}{E}\right)^2 \frac{X}{n} \left(1 - \frac{X}{n}\right) \approx \left(\frac{z_{C.I.}}{E}\right)^2 p(1 - p)$$

$$95\% \text{ C.I.} \Rightarrow z_{95\%} = 1.96$$

$$\text{expected } \frac{X}{n} \approx 0.05 - 0.10 \Rightarrow E \approx 0.025$$

$$\text{"conservative" } p \approx 0.25$$

$$n \approx \left(\frac{1.96}{0.025}\right)^2 0.25(1 - 0.25) \approx 1000$$

$$n \approx \left(\frac{1.96}{0.025}\right)^2 0.5(1 - 0.5) \approx 1500$$



“I was on slashdot.org and found this blog.
AND I’ M UPSET..... I don’ t know why I’ m
upset but I figured since everyone else was
UPSET.... I would be too. How dare you
cause me to be UPSET.... I was happy just
looking at the Longhorn pics and next thing
I know I’ m UPSET..... Why on earth would
anyone be UPSET as me. I didn’ t get my
identity stolen. Heck I don’ t even live in
INDIANA.... Which makes me UPSET.....”

-Blog post by *Anonymous Coward*