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/
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

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

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

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
Motivation

Web

Cybersecurity
Phishing for Clues

Inferring Context Using Cascading Style Sheets and Browser History

Markus Jakobsson, Tom N. Jagatic, and Sid Stamm

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.
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:

<table>
<thead>
<tr>
<th>Description</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of people who visited the site (total)</td>
<td>28</td>
<td>100%</td>
</tr>
<tr>
<td>Number of people who visited the site (unique)</td>
<td>17</td>
<td>60%</td>
</tr>
<tr>
<td>Number of people who submitted queries (unique)</td>
<td>16</td>
<td>57%</td>
</tr>
<tr>
<td>Number of people who proceeded to order (unique)</td>
<td>8</td>
<td>28%</td>
</tr>
<tr>
<td>Number of people who entered credit card information (unique)</td>
<td>1</td>
<td>3%</td>
</tr>
<tr>
<td>Number of people who entered bank account information (unique)</td>
<td>2</td>
<td>7%</td>
</tr>
</tbody>
</table>

© 2005 Filippo Menczer @ Phishing Research Group
Riddle

He starts and ends 2 common English words. One painful in love, One painful in everyday matter. Do you know what 2 words I must be?

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?

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

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 Citital Inc.

Virgil Griffith
Research Assistant at Indiana University and Student at Indiana University

Shouhuai Xu
Professor at University of Texas, San Antonio

Hampus Jakobsson
Marketing Manager at TAT AB and Owner, TAT AB (TAT works with UIs for constrained systems)

Hein R
Computer Scientist and Software Engineer
Virgil Griffith's Profile

**Information**

**Account Info:**
Name: Virgil Griffith
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: griffith@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:
- Will also be around Pasadena for:
  - http://asc.caltech.edu/index.htm

**Friends at Indiana**

Kim Hedge  Marisa Geoghegan  Rebecca McCrigit
Eric Nichols  Jordan DeLong  Michael Amlung

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

**Other Schools**
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: biaspan

4: csci_e_170, csci_e_170a, lj_clients, lj_dev

5: ms_secbulletin, msft_briani, simson_net, techreview, techreview_blog

Friend of: 14: aqaran, anaisdjuna, anotherjen, catya, chanaleh, drqlam, erikin, ivorjawa, kill, marypcb, mr_privacy, silentbamboo, src, xthread

Member of: 4: csci_e_170, csci_e_170a, lj_dev, paidmembers
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.
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 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, May 2005.
Experiment Design

- **Web**: Access from the internet.
- **IU phone book**: Access from the university.
- **Social Network Database**: Access to social context.
- **Social Context Experiment**
- **Control Experiment**

**Emails**

- **From: alice@indiana.edu**
  - **To: bob@indiana.edu**
  - **Subject: This is cool!**
  - **Hey, check this out!**
    - `<A HREF="https://www.whuffo.com/index?bob">www.indiana.edu/~phishing</A>`

- **From: stranger@indiana.edu**
  - **To: charlie@indiana.edu**
  - **Subject: This is cool!**
  - **Hey, check this out!**
    - `<A HREF="https://www.whuffo.com/index?charlie">www.indiana.edu/~phishing</A>`

**Victim Social Group**
- **(487 subjects)**

**Victim Control Group**
- **(94 subjects)**

**Phishing Attacks Using Social Networks**

- **Access & Login Log**
- **whuffo.com**
- **credentials**

**Access**

**Kerberos Authenticator**

**Success**

**Key Distribution Center**

**iu.edu**

**Message Box**

- **!!!!! You must use your Indiana Network ID and Password !!!!!!**
  - **User name:**
  - **Password:**
  - **Remember my password**

**Browser**

- **https://www.whuffo.com/**
Main Result

- Control: 16% ± 7%
- Social: 72% ± 4%
- Social-forward: 53% ± 6%

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

Unique Visits and Authentications per Hour

Repeat Hits

- Repeat Authentications
- Refreshes of Authenticated Users

$X^{-2.5}$

$X^{-1.1}$
Gender Effects

<table>
<thead>
<tr>
<th></th>
<th>To Male</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>From Male</td>
<td>53%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>From Female</td>
<td>68%</td>
<td>78%</td>
<td></td>
</tr>
<tr>
<td>From Any</td>
<td>65%</td>
<td>77%</td>
<td>72%</td>
</tr>
<tr>
<td>To Male</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To Female</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To Any</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Success Rate

From Male: 53%
From Female: 68%
From Any: 65%
To Male: 78%
To Female: 76%
To Any: 77%
More Demographics
More Demographics

![Graph showing success rate by political views](image-url)
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

4/21
Start exp

4/24/2005
• End exp
• Debrief email w/links to site & blog

4/25
65 posts on blog

4/26 (p.m.)

Slashdot

Phishing for Credit

Posted by Zenk 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 would 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 IDS 1st page

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

For students duped by a bogus e-mail claiming to be from the EU server, two students at the School of Informatics have a message: You've been spotted by vicious World Wide Hackers.

The hackers, graduate students Tom Japicke and Mike Johnson, conducted an email 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, Japicke 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 friend Tom@Indiana.edu. The subject would read "This is cool and the e-mail would be signed, "Nice.

"The idea of this e-mail is that 'Hey, check this out!' and provided a link on the EU server that prompted students to provide their username and password. The e-mails were not actually sent from the e-mail accounts they originated from.

"I was deceptive, (but) there was no other way to conduct the study," said Filip Marincek, an associate professor of Informatics and computer science. The study was conducted by Japicke and Johnson as part of Marincek's graduate-level Web mining course offered through the School of Informatics. Associate Professor of Informatics Markus Riedebach was the faculty advisor for the study.

"We feel very bad that the students felt violated. That doesn't mean that it was unethical or illegal," Filip Marincek Information and computer science associate professor

In May...

4/27
Blog closed (440 posts)

4/27 UITS news, KB updated

4/27 IDS Editorial

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

Thanks to your own inattention there to be virtually connected, your passwords for information and services widely available online, legally and illegally, to whoever wants to get it.

Two graduate Informatics students used public Web sites (with access) to help set up an experiment that tested how online connections affect responses to requests for information on the Internet.

While the study is of a vital academic and security nature, the school employed an element in heavy students and secure supporting studies of their research institution, and that support is not compromised when.

4/28 IDS 1st page

In May...

Hackers with hearts of gold
Cybersecurity researchers look like "the bad guys" as they tackle security problems
By Colleen Carter

"Phishing" experiment angers university cybersecurity issues, shortcomings
By Anthony Babjak

"If it's not a phishing attack, the people who are the bad guys look like us," said Anthony Babjak, a professor of computer science at Indiana University.

The study by graduate students in the School of Informatics involved e-mailing students who had been identified as "high performers" online.

The "bait" e-mail included a link to a site that would ask for personal information, such as a Social Security number or username and password. The students were asked to keep track of how many people clicked on the link.

In May...

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/fraudulent/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?

$$C.I. = \frac{X}{n} \pm z_{c.i.} \frac{S_X}{\sqrt{n}}$$

$$E = z_{c.i.} \frac{S_X}{\sqrt{n}} = z_{c.i.} \sqrt{\frac{X}{n} \left(1 - \frac{X}{n}\right) n}$$

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

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

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

"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