

# Social Phishing

By Tom N. Jagatic  
Nathaniel A. Johnson  
Markus Jakobsson  
Filippo Menczer

October 2007/Vol. 50, No. 10 COMMUNICATIONS OF THE ACM

Presented by Zhe Sun (University of Auckland)



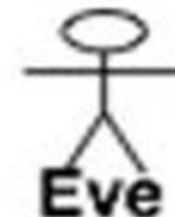
# Summary

- This paper disclose a working theory for social phishing.
- Also show baseline success rate for individual phishing attacks compare with normal phishing from a social phishing experimenting in the Indiana University.

# What is Social Phishing?

- **Social Phishing:** using people's personal information or social contacts (acquaintance's information) to increase the power of phishing.

From: Alice@indiana.edu (spoofed by Eve)  
To: Bob@indiana.edu  
Subject: This is Cool!



Hey, check this out!

<https://www.indiana.edu/%7e%70hi%73%68%69n%67...>

Alice

# What is Social Phishing and How it works?

- **Information Gathering from public**

- **social network sites:** Make friend network (Friendster (friendster.com), Facebook(facebook.com).....). Online blogging communities. (LiveJournal (livejournal.com), is the Friend of a Friend (FOAF) project) etc.
- Allow a phisher to harvest large amounts of **reliable social network information** from above websites with particular tools.

- **Sending Email**

From: Alice@indiana.edu (spoofed by Eve)  
To: Bob@indiana.edu  
Subject: This is Cool!



Hey, check this out!

<https://www.indiana.edu/%7e%70hi%73%68%69n%67...>

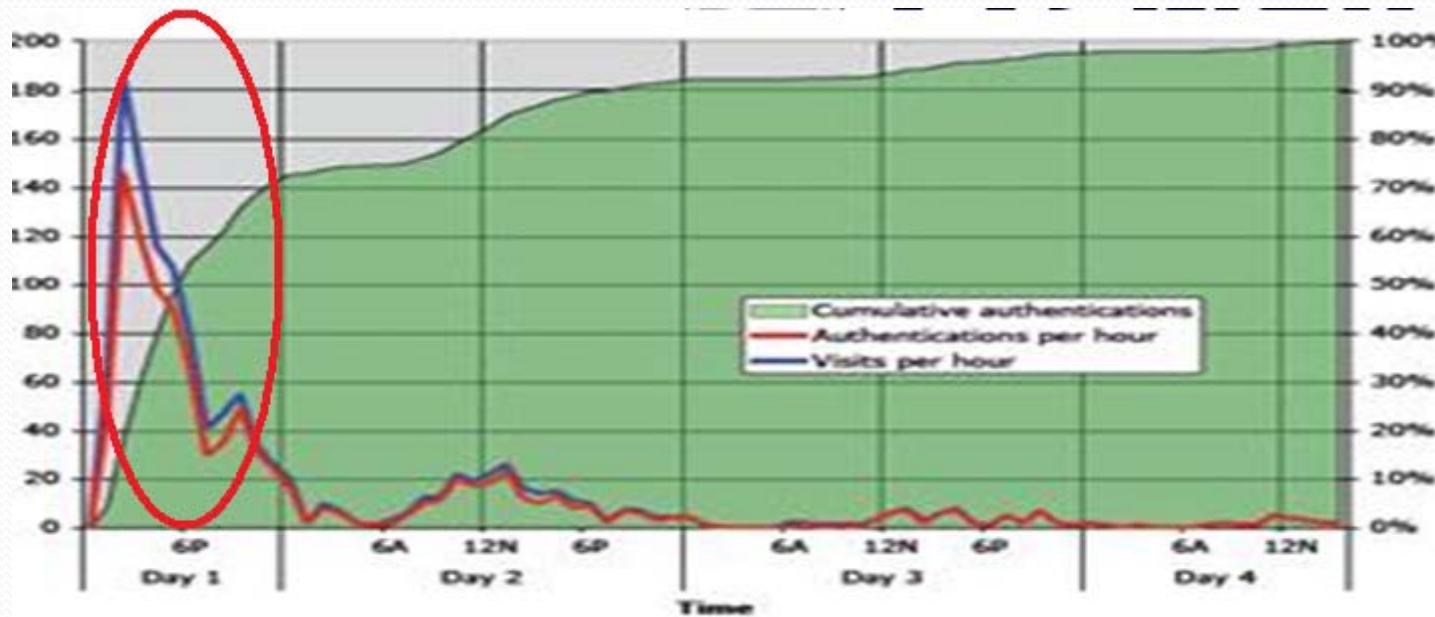
Alice

- **Use fake website get information**

- University Login page, Online Banking login page etc.

# Appreciate Comment

- This paper shows Social phishing is efficient to get Internet user's authentication information

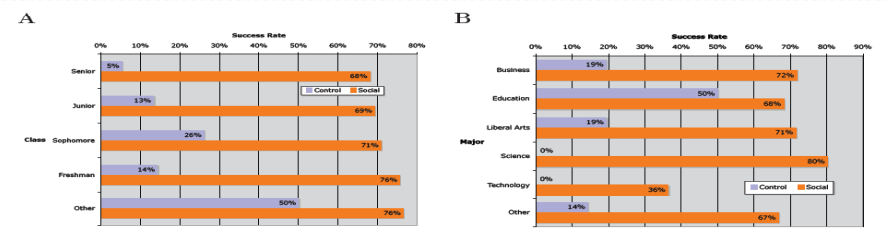
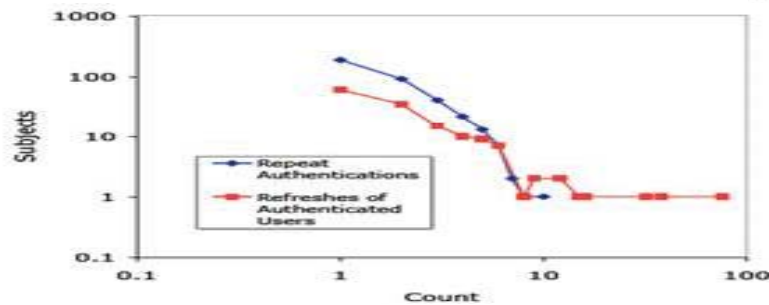


70% of successful authentication occurred in first 12 hours

# Criticises

- List lots of useless or less meaning record confuse readers

	Successful	Targeted	Percentage	95% C.I.
Control	15	94	16%	(9-23)%
Social	349	487	72%	(68-76)%



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

- List Unreliable data to make things seems significant

<https://www.indiana.edu/%7e%70hi%73%68%69n%67...>



# Question and discussion



The University of Auckland  
NEW ZEALAND



**EC Mail**  
webmail interface



Notices and News

**We will never ask for your password. Ever.**

Recently there have been some phishing attempts on campus.  
Emails claiming to be from the University or a University system asking for your name, password or other personal information.  
We will never ask for your password. Ever. These are false emails.  
If in doubt contact your local support person..

- **Anti-Phishing suggestions from the author:**
  - Digitally signed email
  - Browser toolbar and some new technique alerted victims before get into phishing website.
- **What's do you think the university need to do when we face Social Phishing attack?**