Social Engineering

COMP620

"A single spear-phishing email carrying a slightly altered malware can bypass multi-million dollar enterprise security solutions if an adversary deceives a cyber-hygienically apathetic employee into opening the attachment or clicking a malicious link and thereby compromising the entire network."

James Scott

COMP620 Schedule

Monday, October 15 Lecture on Phishing	Wednesday, October 17 Review for exam	Friday, October 19 Second Exam
Monday, October 22 Exam returned Last day to drop	Wednesday, October 24 Guest lecture on Malware Analysis	

Social engineering

- **Social engineering** is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques
- Similar to a confidence trick or simple fraud

Users Often Make Bad Decisions

- Many naive users will OK anything
- Many users have insecure passwords
- Most users do not know how to protect their computer

Phishing

- Phishing is the criminally fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity
- Targeted versions of phishing have been termed **spear phishing**

Types of Phishing

- **Spear Phishing** – Targeted at specific individuals or companies
- **Whaling** – Attacks directed specifically at senior executives and other high-profile targets
- **Clone phishing** – A legitimate email whose attachment or link has been replaced with malware. It is often sent with a spoofed return address of the original source

Phishing Effectiveness

- 95% of all attacks on enterprise networks are the result of successful spear phishing.
- phishing attempts have grown 65% in the last year.
- 76% of businesses reported being a victim of a phishing attack in the last year.
- 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link.
- nearly 1.5 million new phishing sites are created each month.

https://blog.dashlane.com/phishing-statistics/

Cost of Phishing

- From October 2013 to December 2016, the FBI investigated just over 22,000 of these incidents involving American businesses
- In total, they saw losses approaching $1.6 billion. That's roughly $500 million every year

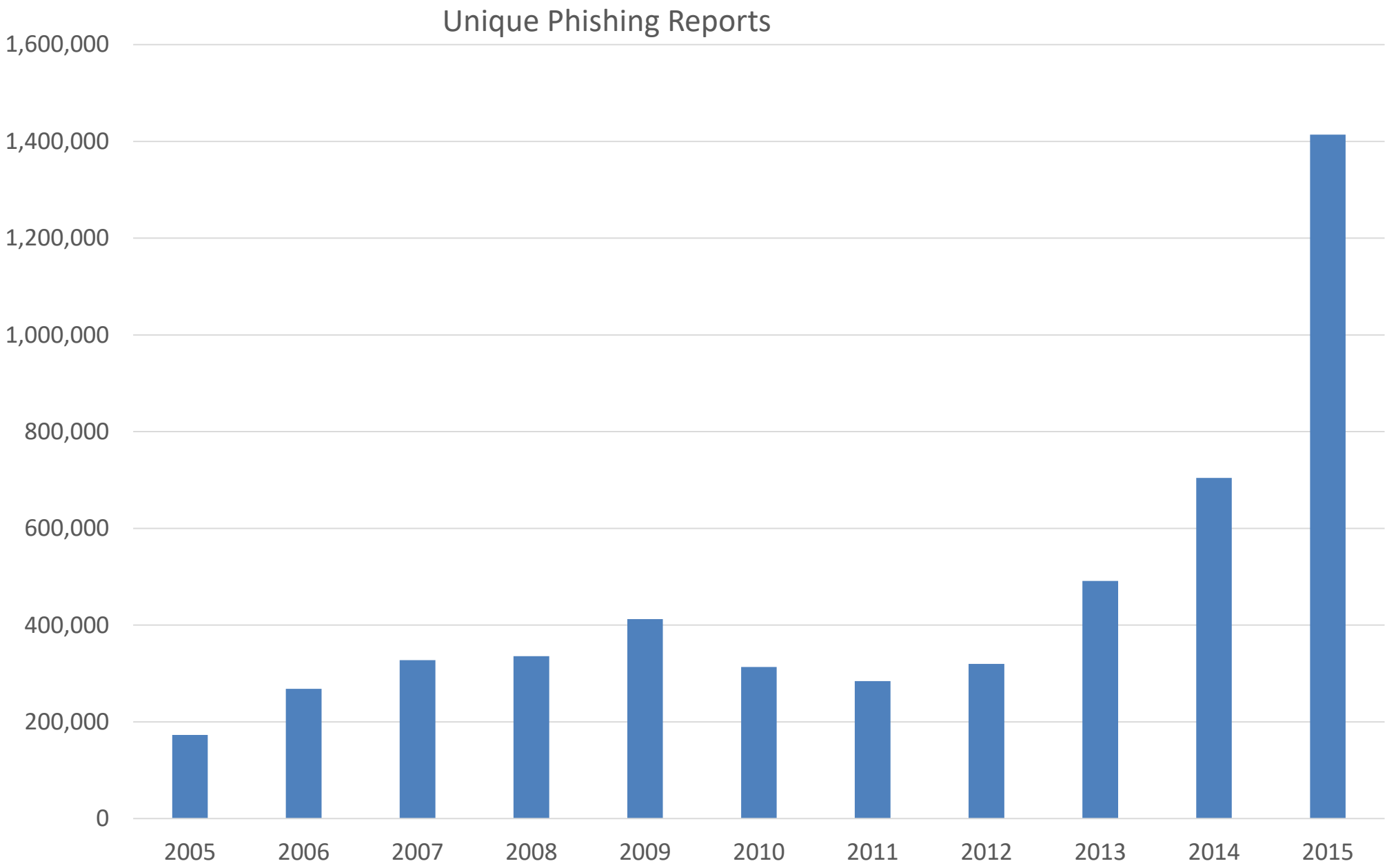
Forbes.com

Social Engineering on Social Networks

- Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft
- In late 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details
- Experiments show a success rate of over 70% for phishing attacks on social networks

History of Phishing

- A phishing technique was described in a paper to the 1987 International HP Users Group, Interex
- In the mid-1990s phishing attacks were made against AOL
- The first known phishing attack against a retail bank was reported in September 2003
- In May 2017, the WannaCry ransomware attack is suspected of having impacted more than 230,000 people in 150 countries


Unique Phishing Reports
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015

Non-Computer Phishing

- An attacker can call someone masquerading as their bank and ask for information
- The attacker can send a text message directing the victim to call a number to resolve an issue
- Known as SMS phishing or smishing
- On March 9, 2012, there were a large number of scam texts that offered a nonexistent $1,000 gift card as bait

Email Phishing

I am the son of a late Nigerian banker. I have inherited the sum of $40 million dollars which I need to transfer to an account in a U.S. bank. If you would assist me in transferring these funds, you would be rewarded with 10% of the amount. Just send me your account number and I will transfer the money to your account.

Email Phishing

The First National Bank is implementing new security features. To keep your account safe, please reply to this email giving:

your account number: _____

your password: _____

You will not be able to access your account in the future unless you provide this information.

More Convincing Email Phishing

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

From my Email Inbox

The Bucks Exchange Server Mailbox Manager has performed an automated cleanup of your junk and deleted items and removed any objects older than 30 days.To remove this limitation and initiate your Account Update process, please click on the link to complete the form.
CLICK HERE:
Click on the link above (or copy and paste the URL address into your web browser).

Thank you for co-operation
WEBMAIL MANAGEMENT TEAM.

The link goes to:
https://www.vizzualforms.com/f/WQR4PykSK60KhU14

Your Experience

- What was the most interesting phishing attack you have seen?

Email Links

- The URL shown in an email link does not have to match the URL used when you click on the link

```
<a href="http://www.evil.com">
  www.nice.com</a>
```

- This displays as

www.nice.com

- In the lower left hand corner of most browsers you can preview and verify where the link is going to take you
- Most phone browsers do not provide this feature

Ken Williams' Opinion

- Browsers and Email systems should warn users when the displayed link does not match the actual URL

Website Forgery

- It is easy to copy the content of a real website and put it on your own fake website
- If the fake website has a digital certificate, it will validate under HTTPS
- Some attackers create websites with very similar names to trusted sites hoping the user won’t notice
- The link www.trusted.evil.com may fool users thinking they are going to www.trusted.com but they are going to evil.com

Man in the Middle Attacks

- A false website can redirect all of the traffic to the true website after recording accounts and passwords
- A Universal Man-in-the-middle Phishing Kit, discovered by RSA Security, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site

Cross Site Scripting Phishing

- If an attacker can put script in something that will be displayed on another user's browser, the script can redirect the user to a malicious website
- The malicious website can be formatted to look exactly like the real website
- Since the user originally started at the legitimate website, they will believe they are on the correct website
- Information entered on the malicious website can be passed to the legitimate website

Countering Phishing

- Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures
- User education is the primary solution
- The secure site “padlock” is becoming more obvious

Filter Evasion

- Some phishing emails put their message in a graphics file
- Humans easily read the message in the picture, but email security scanners often do not recognize the message
- Some email security systems use Optical Character Recognition to check for text in images
- Some websites hide phishing-related text using Flash, a technique known as “phlashing”

Click Through Syndrome

- Many users will allow a dangerous event to occur because it appears necessary to make the activity work
- This is exacerbated by poorly managed honest sites that have certificate problems

Recognizing Phishing

- Phishing emails from other countries often have poor grammar
- The source of the email should be the expected organization
  - Source might be obscured
  - Reply all may show correct sender
- A valid email is going to have you contact or link to a site within the organization
- Check if a link goes where it should
- Real emails will know about you (i.e. name, credit card)

What is wrong with this?

to: info@notice.com
from: Fulton, Amy [amy.fulton@ubc.ca]
subject: Information 2:4:7 Needed Urgent

Dear Email user,

Your mailbox has exceeded storage limit set by your administrator. You may not be able to send or receive new mail until your mailbox size is increased by our helpdesk administrator. To increase your storage limit,
CLICK HERE

You will continue to receive this warning message periodically if your inbox size continues to exceed its size limit. This email is intended only for the use of the individual or entity to which it is addressed and contains information that is privileged and confidential.

Thank you for your cooperation.

Webmail Help Desk
System Administrator

Clues

to: info@notice.com
from: Fulton, Amy [amy.fulton@ubc.ca]
subject: Information 2:4:7 Needed Urgent

Dear Email user,

Your mailbox has exceeded storage limit set by your administrator. You may not be able to send or receive new mail until your mailbox size is increased by our helpdesk administrator. To increase your storage limit,
CLICK HERE

You will continue to receive this warning message periodically if your inbox size continues to exceed its size limit. This email is intended only for the use of the individual or entity to which it is addressed and contains information that is privileged and confidential.

Thank you for your cooperation.

Webmail Help Desk
System Administrator

Office 365 ATP Safe Links

- Used at A&T to check links in emails
- When email arrives at an Exchange email server, it modifies links in the email to connect to a Microsoft Safe Links server
- If the Safe Links server believes the website to be safe, it redirects you connection to the desired web server
- If the link is on a list of suspected web sites, an error message is displayed
- Part of Microsoft's Advanced Threat Protection (ATP)

Augmenting password logins

- Some sites display a personalized phrase when you are asked to enter your password
- If you do not see the correct phrase, you should not enter your password
- The sites IP address can be used as part of the user authentication

Legislation

- Federal laws have been proposed to fight phishing
- Senator Patrick Leahy introduced the Anti-Phishing Act of 2005 in Congress on March 1, 2005
  - Criminals who created fake web sites and sent bogus emails in order to defraud consumers to fines of up to $250,000 and prison terms of up to five years
  - It did not pass

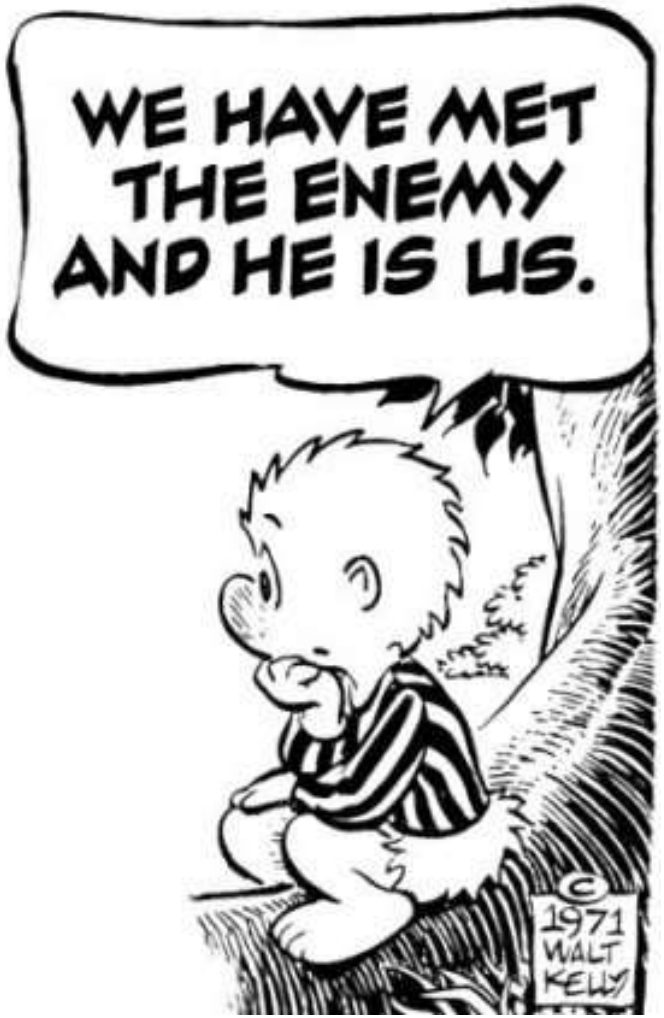
Legal Remedies

- On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected phisher, a Californian teenager, who created a webpage to look like the AOL website, and used it to steal credit card information
- He was found guilty of sending thousands of e-mails to America Online users, while posing as AOL's billing department

Public Service Announcement

https://en.wikipedia.org/wiki/Phishing

Computer users are often the greatest threat to their own system security.



COMP620 Schedule

Monday, October 15 Lecture on Phishing	Wednesday, October 17 Review for exam	Friday, October 19 Second Exam
Monday, October 22 Exam returned Last day to drop	Wednesday, October 24 Guest lecture on Malware Analysis	