Combating Phishing Attacks: A Never Ending Arms Race?

Norman Sadeh
School of Computer Science
Carnegie Mellon University

Work conducted in collaboration with:
Lorrie Cranor, Jason Hong, Alessandro Acquisti, Julie Downs,
Sven Dietrich, Anthony Tomasic, and many graduate students

Outline
- What is Phishing?
- How big of a problem is it?
- What are the current solutions?
- Carnegie Mellon University’s research on “Supporting Trust Decisions”
  - Largest US research projects on combating phishing attacks (2005-present)
  - Multi-pronged approach
  - Studies and existing deployments
- Concluding Remarks
- Q&A

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don’t re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?Signin

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend,
Phishing is a Plague on the Internet

Phishing sites reported in Nov 2007: ~28,000 unique sites.

Phishing losses a year (sources: Google & Garf): ~$350m-$3b (does not include damage to brand, sales, etc.)

...Just the tip of the iceberg...

Spear Phishing

- Phishing attacks also used for espionage
  - Government (e.g. IRS, Medicare/Medicaid, DoD)
  - Corporate, incl. pharmaceutical
    - Recent Salesforce.com phish
    - Recent trend in targeting executives

...Spear Phishing Attacks...

Major corporations and their vendors too!

...and More...

- SMiShing – SMS phishing
  - Example: “We’re confirming you’ve signed up for our dating service. You will be charged $2/day unless you cancel your order.”
  - When user clicks on the link, malware is installed

- Vishing – VoIP phishing
  - Exploits caller ID spoofing
  - Instruct user to call a number and provide personal details

- Social networks
Why do people fall for phishing attacks?

Little knowledge of phishing

- Only about half knew meaning of the term “phishing”

"Something to do with the band Phish, I take it."

Minimal knowledge of lock icon

- Only 85% of participants were aware of lock icon
- Only 40% of those knew that it was supposed to be in the browser chrome
- Only 35% had noticed https, and many of those did not know what it means

"I think that it means secured."
"It symbolizes some kind of security, somehow."

Copyright © Lorrie Cranor, Jason Hong & Norman Sadeh, 2006-2008
Little attention paid to URLs

- Only 55% of participants said they had ever noticed an unexpected or strange-looking URL
- Most did not consider them to be suspicious

“If it wasn’t one of my standard dot-com, dot-edu, dot-us or some country code, then I would be really curious what that meant.”

Some knowledge of scams

- 55% of participants reported being cautious when email asks for sensitive financial info
- But very few reported being suspicious of email asking for passwords
- Knowledge of financial phish reduced likelihood of falling for these scams
- But those knowledgeable about financial phish were not necessarily suspicious of other scams, such as amazon.com password phish

Naive evaluation strategies

- The most frequent strategies don’t help much in identifying phish
  - This email appears to be for me
  - It’s normal to hear from companies you do business with
  - Reputable companies will send emails

“I will probably give them the information that they asked for. And I would assume that I had already given them that information at some point so I will feel comfortable giving it to them again.”

Past experience helps some

- Those who had seen scams in the past could identify similar scams
  - All but one participant correctly identified a Katrina email message as a scam
- But knowledge of some scams didn’t seem to help them identify other types of scams
Today’s Solutions Fall Short

Today’s Solutions - in a Nutshell

- Public Key Infrastructure or multi-factor authentication
  - People don’t understand certificates
  - Secure sign-on, using pictures and passphrases
- Usability: people don’t notice/ignore

Anti-phishing filters that rely on blacklists and whitelists
  - Always one step behind & possible liability

Some training – e.g. websites, posters
  - Users just don’t pay attention

Protect Yourself from Fraudulent Emails

What is a fraudulent email?

A fraudulent (spoof) email pretends to be from a well-known company, such as eBay, in an attempt to get personal information from you. People are often fooled into opening the email, responding, or clicking links, which can reveal personal information such as credit and debit card passwords – to commit identity theft.

You can prevent spoof from affecting you
Today’s Solutions - in a Nutshell

- **Spam filters** have limited success catching phish
  - In contrast to spam, phishing emails look legitimate

What else can we do?

Multi-Pronged Approach

- **Human side**
  - Interviews to understand decision-making
  - Embedded training
  - Anti-phishing game

- **Computer side**
  - Email anti-phishing filter
  - Automated testbed for anti-phishing toolbars
  - Anti-phishing toolbar

- **Automate where possible, support where necessary**

PILFER Email Filter

- **Rationale**: Spam filters let a large number of phishing emails slip through
- **Solution**: Phishing email filter combining a set of features aimed at catching deception along with **advanced machine learning** techniques
- Can work in **standalone** mode or as **complement to spam filter**
  - e.g. available as SpamAssassin plugin

---

*Copyright © Lorrie Cranor, Jason Hong & Norman Sadeh, 2006-2008*
PILFER: Approach

- **Features intended to detect deception**
  - Emails are made to look like legitimate emails from the company, so text analysis is of limited value
- **Included features:**
  - Age of linked-to domains
  - Number of domains linked to
  - Presence of attention-directing links ("click here") that link to a domain other than the most common one in the email
- Trained using **Random Forests**

CANTINA Web Page Filter

- **Rationale:** Blacklists fall short
  - Always one step behind
  - Only protect from most common attacks, i.e. no spearphishing protection
  - Easily overcome by criminals
- **Solution:** Uses a content-based approach
  - Lexical signature & PageRank to identify phishing sites
  - Highly effective
  - No human intervention required
  - Protects against spearphishing

CANTINA: Phishing Web Site Detector

- **CANTINA uses a simple content-based approach**
  - Examines content of a web page and creates a "fingerprint"
    - Uses TF/IDF
  - Sends that fingerprint as a query to a search engine
  - Sees if the web page in question is in the top search results
    - If so, then we label it legitimate
    - Otherwise, we label it phishing
  - Some additional heuristics
- **Nice properties:**
  - Fast
  - Scales well
  - No maintenance by us (done by search engines)
  - Highly accurate

Copyright © Lorrie Cranor, Jason Hong & Norman Sadeh, 2006-2008
Evaluating CANTINA (Iteration #2)

Anti-Phishing Phil Game

- **Rationale**: Traditional training doesn’t work
  - But people do like playing games
- **Solution**: A game teaching about phishing

Results with **tens of thousands** of users show:
- People more willing to play game than read training
- People better at identifying phishing sites after playing


Copyright © Lorrie Cranor, Jason Hong & Norman Sadeh, 2006-2008
Good job spotting numbers in the URL.

Don't trust URLs with all numbers in the front.
More about the game

- Four rounds
  - Increasing difficulty
  - Two minutes in each round
- Eight URL “worms” in each round
  - Four phishing and four legitimate URLs
  - Users must correctly identify 6 out of 8 URLs to advance

User Study

- Test participants’ ability to identify phishing web sites before and after training
  - 10 URLs before training, 10 after, randomized
  - Up to 15 minutes of training
- Three conditions:
  - Web-based phishing education
  - Tutorial
  - Game
- 14 participants in each condition
  - Screened out security experts
  - Younger, college students
Falling for Phishing

- Misidentifying Legitimate Sites

Results

- No significant difference in false negatives among the three groups
- Game group performed best in false positives
- Game condition performed best in total correctness
- The training material made people paranoid but not more effective!

PhishGuru Embedded Training

- **Rationale**: Existing training doesn’t work
- **Solution**: Tool to train people during their normal use of email
  - Periodically, insert fake phishing emails in people’s regular mail
  - If person falls for it, **intervention warns and trains user** in succinct and engaging format
  - Provide reports to help companies **assess their preparedness levels**
  - Can be customized for individual orgs.

---

Comic Strip Intervention

PhishGuru: Evaluation

Status Today

Concluding Remarks

- Social engineering is not a new phenomenon
- Unfortunately, with the Web, it can be carried out on a much larger scale and much more cheaply
- Phishing: A never-ending arms race?
- Many large organizations (private and government) are extremely concerned
- As technology evolves and as users become more aware of potential attacks, the attacks will continue to evolve

Phishing: A never-ending arms race?
References


Acknowledgement: A number of the slides used in this presentation have been adapted from presentations developed by or with my collaborators in this project. This includes Lorrie Cranor, Jason Hong, Julie Downs, Ponnurangam Kumaraguru, Ian Fette and Steve Sheng.