Security Skins: Embedded, Unspoofable Security Indicators

Rachna Dhamija
Center for Research on Computation and Society
Harvard University
Talk Outline

- Why Phishing Works
- Dynamic Security Skins
- Embedded Security Indicators
• Why Phishing Works
  Dhamija, Tygar & Hearst, CHI April 2006
• Dynamic Security Skins
• Embedded Security Indicators
PayPal - Login

Welcome | Send Money | Request Money | Merchant Tools | Auction Tools

Member Log In

Registered users log in here. Be sure to protect your password.

Email Address: | Password: | Forget your email address? | Forget your password?

New users sign up here! It only takes a minute.

Log In

About | Accounts | Fees | Privacy | Security Center | Contact Us | User Agreement | Developers | Jobs | Buyer Credit | Referrals | Shops | Mass Pay

PayPal, an eBay company

Copyright © 1999-2005 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Goals of Our Study

• To design anti-phishing solutions, we need to understand:
  – Which attack strategies work?
  – Who gets fooled
  – Why?
The goal was to discover knowledge and skills required by users

We evaluated 200 phishing attacks from APWG archive

From this, we developed a set of hypotheses for why users are fooled
Hypotheses

Why users are fooled by attacks:

1. Lack of Knowledge
   a) Computer system knowledge
   b) Knowledge of security & security indicators

2. Visual Deception
   a) Visually deceptive text
   b) Images masking underlying text
   c) Images that mimic browser chrome
   d) Windows masking underlying windows
   e) Deceptive look and feel

3. Bounded Attention
   a) Lack of attention to security indicators
   b) Lack of attention to the absence of security indicators
Usability study: how do participants distinguish legitimate websites?

- We archived 200 phishing websites
  - 2 months phishing email from colleagues
  - 1 week of phishing email from MailFrontier

- We showed participants 19 websites in random order
  - 7 legitimate websites
  - 9 phishing websites
    - with varied domain name, type of request, phishing techniques
  - 3 constructed phishing attacks
    - (popups, spoofed SSL indicators, …)
    + 1 website that presents a self-signed certificate

- Websites were fully functioning
  - Several levels deep, same domain name, links, etc.
Study Design

• Within-subjects design

• Scenario:
  Imagine that you receive an email message that asks you to click on one of the following links. Imagine that you decide to click on the link to see if it is a legitimate website or a "spoof" (a fraudulent copy of that website).

• Talk Aloud study- participants were asked:
  – Is this site legitimate?
  – Reasoning & confidence level
  – Would you give data?
  – Have you been to this website or have account?

• Participants primed to look for spoofs
  – No deception
  – Spoof detection rate higher than real-life
  – If our participants are fooled, real users will be too
Participants

• 22 participants
  – 45% male, 55% female
  – Age 18-56
  – 50% staff, 50% students
    • Staff: 73% Bachelors, 18% Masters, 9% J.D.
    • Students: 67% Masters, 18% Masters, 18% Ph.D.
  – 86% non-technical, 14% technical
  – Used a variety of OS, browser & email
• Recruited by XLab (university service)
• $15 participation fee
Study Results: Participant Score

Number of Websites Judged Correctly by Each Participant (out of 19 websites)
Study Results: Website Difficulty

Difficulty of Each Website

- Fake Bank Of the West (bankofthevwest.com)
- Fake Paypal (XUL-based spoof)
- Real Etrade (everypath.com)
- Fake Paypal (paypal-signin03.com)
- Fake Paypal (IP address)
- Real Capital One Login Page
- Fake Paypal (screenshot of SSL indicators)
- Fake Ameritrade (ameritrading.net)
- Fake Bank of America (w/ popup window)
- Fake Bank Of The West (IP address)
- Fake USBank (IP address)
- Fake Ebay (IP address)
- Fake Yahoo(center.yahoo-security.net)
- NCUA (IP address)
- Real Ebay
- Real Bank Of America
- Real Telebears
- Real PayPal
- Real Bank One

Percent of Participants
Study Results: Confidence Level When Correct

![Bar Chart showing confidence levels for various websites and services]
Participants are confident, whether correct or incorrect.
Spoof- www.bankofthevvest.com

- 91% incorrect
- 68% would give data
- Convinced by:
  - “cute” animation
  - Links to legit pages
    • Consumer alert
    • Verisign logo

Consumer alert

- Verisign logo
50% incorrect
81% incorrect
Welcome to Capital One Savings Online Service
Please enter your account identification information below.

User ID
Password

Log In

Forgot your password?

If you are a deposit customer of Capital One Bank or Capital One, F.S.B., you may register for Capital One Savings Online Service.

Trouble signing in? Contact Customer Support or call 1-800-559-0232.

Privacy | Security | Terms and Conditions
Capital One Bank, Capital One, F.S.B., members FDIC.
©2005 Capital One Services, Inc.
Capital One is a federally registered service mark.
All rights reserved.

50% incorrect
Self-signed SSL Certificate

Unable to verify the identity of cardea.sims.berkeley.edu as a trusted site.

Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be cardea.sims.berkeley.edu, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to accept this certificate for the purpose of identifying the web site cardea.sims.berkeley.edu?

Examine Certificate...

- Accept this certificate permanently
- Accept this certificate temporarily for this session
- Do not accept this certificate and do not connect to this web site

- 15 participants selected “OK” without reading
- 3 read & selected “OK”, 2 chose “do not accept”, 2 examined cert
- When asked what warning was about:
  - 18 didn’t know, 3 were incorrect (cookies, passwords, spyware)
  - only 1 was correct
Certificates

Only 1 participant could explain the certificate.
What determines participant score?

• Score was not significantly associated with
  – Sex
  – Age
  – Level of education
  – Hours using the computer
  – Previous use or account with website

• Participant knowledge and use of security indicators was a more important factor

• We categorized participants into strategy types based on their behavior and responses to our interview questions
Strategy Type 1 performed significantly worse than other types.
Strategy 1: Security Indicators in Website Content

5 participants (23%):

- Don’t look at address or status bar

- Don’t use URLs
  - “I never look at the letters and numbers up there. I’m not sure what they are supposed to say”.
  - Can’t distinguish different sites

- Rely on images, logos, links and security warnings
  - “Why would a phishing site have a phishing warning?”
Strategy 2: Website Content & Address Only

8 participants (36%):

- Notice IP address
- Notice when domain changes
- Don’t notice SSL indicators
Strategy 3: Content & Address + HTTPS

2 participants (9%):

- Can distinguish HTTP & HTTPS
- Don’t use SSL lock icon in status bar
  - “It is too far away and out of my peripheral vision”
5 participants (23%): 

- Use website content, address, https and lock icon
Strategy 5: Also Check Certificates

2 participants (9%):

- Use content, address, SSL indicators, and also check certificates.
Additional Strategies

• 2 participants were only suspicious if more than password and username were requested
  – 1 entered usernames and passwords to see if she had an account (in study & real life)
    • “What’s the harm? Passwords are not dangerous to give like money information is” (Type 1, Score 7)

• 1 participant confirmed every website by Yahoo search (Type 4, Score 18)
Why users are fooled by attacks:

1. Lack of Knowledge
   a) Computer system knowledge
   b) Knowledge of security & security indicators
   c) Knowledge of web fraud
   d) Erroneous security knowledge

2. Visual Deception
   a) Visually deceptive text
   b) Images masking underlying text
   c) Images that mimic browser chrome
   d) Windows masking underlying windows
   e) Deceptive look and feel

3. Bounded Attention
   a) Lack of attention to security indicators
   b) Lack of attention to the absence of security indicators
Summary of Results

- Even though participants were informed & motivated, good phishing sites fooled 90%

- Existing anti-phishing browsing cues are ineffective.
  - Cues are not noticed
    - 60% ignored SSL indicators
    - 68% clicked OK on warning notice w/o reading
  - Cues are not understood
  - Cues are trivial to spoof
Conclusions

- We need a different approach for usable security design
  - Security is a secondary goal
  - Users misplace trust in logos and indicators
  - Assume that uniform graphic designs will be copied!
  - Indicators placed in the periphery may be ignored
  - Designers should “spooﬂ” own designs in user testing
Talk Outline

• Why Phishing Works
• Dynamic Security Skins
• Embedded Security Indicators
• Why Phishing Works
• **Dynamic Security Skins**
  Dhamija & Tygar, SOUPS 05
• Embedded Security Indicators
Review: Password Authenticated Key Exchange

- Many protocols exist (EKE, SPEKE, SNAPI, AuthA, PAK, SRP, etc…)
- The paper discusses one, SRP
Many protocols exist (EKE, SPEKE, SNAPI, AuthA, PAK, SRP, etc…)
The paper discusses one, SRP
Review: Password Authenticated Key Exchange

- Many protocols exist (EKE, SPEKE, SNAPI, AuthA, PAK, SRP, etc…)
- The paper discusses one, SRP

Summary of advantages of SRP:
- user authentication & mutual authentication
- preserve familiar use of passwords
  - secret stored in memory of the user
  - user doesn’t need a trusted device
- no passwords sent over the network
- server doesn’t store password
But protocols alone won’t stop phishing!

Password entry mechanism can be spoofed.
• Preserve familiar use of passwords

• User must be able to verify password prompt, before entering password

• Rely on human skills
  – To login, recognize 1 image & recall 1 password (for any # of servers)
  – To verify server, compare 2 images

• Hard to spoof security indicators
Dynamic Security Skins Password Window

- Mozilla Firefox extension
- Trusted window, dedicated to password entry
- Trusted path ➔ one-time customization
- Random photo assigned or chosen
- Image overlaid across window
  - and over textboxes
- User recognizes image first
  - then enters password
- Password not sent to server
Usability Study

- Think aloud, informal study
  - Do users understand concept?
  - Can users enter password?
  - Will users check images?
  - Do users notice spoofs?

- Step 1: Select *personal image*
Password Window Displays Personal Image

Berkeley Bank requires a username and password:

Username:
Password:

Login  Cancel
Password Window & Website Display Image

Please update your credit card billing address:

- **NAME**: [Input Field]
- **CREDIT TYPE**: Visa [Drop-down]
- **CREDIT CARD #**: [Input Field]
- **EXPIRATION DATE**: [Input Field]
- **BILLING ADDRESS**: [Input Field]

[Submit Button]
Spoofing the Password Window

Different personal image

No personal image
Results

- Users love personal images
  - “Can I use my own image?”
  - Only one (technical) user dissatisfied
  - DSS appreciated most by naive users

- All users could enter password only when personal image was shown

- All users recognized when different personal image was presented

- All users recognized when no image was presented
  - But some users confused (e.g. “The software isn’t working”)
  - One user entered in two characters of password before realizing

- Users could perform pattern matching
  - Users said it was very easy, but some said they will not always check
  - “It is kind of fun, but after a while I might ignore it. I might only check it if I was concerned or if it was my bank”

- Motivated design improvements…
Design Improvements: Reduce Footprint
Display of Dynamic Patterns on Website

• Integrate w/ website design

• e.g., Embed skins in brand logos

PayPal
Talk Outline

• Why Phishing Works
• Dynamic Security Skins
• Embedded Security Indicators
• Why Phishing Works
• Dynamic Security Skins
• Embedded Security Indicators

Harvard Security Usability Class Project (Ian Fischer, Philip Hendrix, Joseph Barillari, Geoffrey Werner Allen)
Spoof Proof Security Indicators

- We are exploring the security skins approach to display other security information in a spoof-proof way:
  - Identity
    - Website
    - Certificate Authority
  - Encryption
    - SSL
    - PAKE
  - Trust Judgments
    - Extended Validation Certificates
    - Whitelist/Blacklist
    - Third Party Recommendations
  - History
    - User history with website (last login, form submission)
    - Site history (e.g., DNS registration)
Embedded Indicators- Form Submission History
Embedded Indicators- Form Submission History
Embedded Indicators - Form Submission History
Participants were interviewing for a job within a company where they would have to manage two credit cards by responding to email notices. A separate email account populated with credit card emails was created for each participant. A proxy was used to mimic legitimate Citibank sites as well as our simulated phishing sites. Participants were asked to process each email in their inbox. They were informed that they should “be careful” with the financial information, but there were no other explicit warnings of the potential for phishing. 3 of the 10 emails were phishing attacks (4, 7, and 9). 22 participants: 10 Control, 12 ESI, 10 male, 12 female, 12 Masters, 1 JD, 2 BA, 8 undergraduates, 18-40 years old, 1 color blind person.
Conclusions

- Users pay attention to indicators within their locus of attention
- Users enjoy the use of shared secret images
- Users can easily recognize their secret image, always recognize false image spoofs and can be trained to recognize that no image is not a bug.

- Challenges
  - Requires secure storage and display of the secret image in browser
  - Reduces portability
  - Phishers can simulate error conditions
  - Spyware and keyloggers