

Why Phishing Works

Rachna Dhamija, J.D. Tygar, Marti Hearst

Presented By: Vince Zanella

Motivation

- To shield users from fraudulent websites, website designers must know which attack strategies work and why
- Hypotheses exist, but no empirical evidence
- Quick numbers: Top phishing sites have tricked upwards of 5% of their recipients into providing them with sensitive information
- Classic Question: What makes a website credible?

This Paper: What Makes a *FRAUDULANT* Website Credible?

- Very interesting space to explore for user-interface designers
- Both phishers and anti-phishers are doing battle in this same space
- But wait, there are already several security measures built into the browser to defeat phishers!

The Empirical Study: A Usability Test

- 22 Participants were showed 20 different websites
- Good phishing sites: 90% fooled
- Existing anti-fishing cues: ineffective
- Average rate of mistakes: 40%
- Popups warning of fraudulent certificates: ineffective
- Participants vulnerable across all backgrounds

Exploit Strategies

- **Lack of Knowledge**
 - Lack of computer system knowledge
 - Lack of security indicator knowledge
- **Visual Deception**
 - Visually deceptive text
 - Images masking underlying text
 - Images mimicking windows
 - Windows masking underlying windows
 - Deceptive look and feel
- **Bounded Attention**
 - Lack of attention to security indicators
 - Lack of attention to absence of security indicators

The Test: Details

- Users were presented with financial and e-commerce websites; some were real, some were spoofs
- Participants task was to identify legitimate and fraudulent websites and give reasoning
- Participants were primed to look for tipoffs
- Note: Study did not look at email lures; instead focused on website security

More Details

- 200 real phishing sites surveyed – a sample of 9 chosen that were representative of the different attack vectors; 3 additional spoof sites created; 7 legitimate sites chosen
- Participants each saw all websites, but in randomized order
- Used Mozilla Firefox 1.0.1 running on Mac OS X
- 20th website in the group was the same for all participants -> required users to accept a self-signed SSL certificate

Demographics

- 45% Male
- Age: 18 – 56, Mean: 29.9, StdDev: 10.8
- Half university staff, half university students
- 14% in technical field
- Primary Browser: 50% IE, 32% FF, 9% Mozilla Unknown, 5% Safari
- Computer Usage Hours per Week: 10 – 135, Mean: 37.8, StdDev: 28.5

Results

- Score: raw number of correctly identified sites: 6
– 18, Mean: 11.6, StdDev: 3.2
- No statistical correlation with a single demographic

Strategies Employed

- **Type I (23%):**
 - Used only content of a webpage to authenticate
 - Confirmed they never looked at the address bar, and didn't actually know what its purpose was
 - Scored the worst (6,7,7,9,9)
- **Type II (36%):**
 - Used content and domain name only
 - Still did not look for any SSL indicators, but were aware of address bar changing
 - Distinguished IP addresses from domain names in address bar
- **Type III (9%):**
 - Used content and address bar, plus https
 - Still didn't look for other SSL indicators, like the padlock
 - Some incorrectly identified site icons (favicons) as security features that cannot be duplicated
- **Type IV (23%):**
 - All of the above, plus the padlock
 - Still, some users gave high credence to a padlock within a page's content
- **Type V (9%):**
 - Everything above, plus certificates
 - Occasionally check certificates when presented with a warning

The Toughest Phishing Site to Detect

- Spoof of Bank of the West's site
- Hosted at www.bankofthevest.com, instead of the legitimate www.bankofthewest.com
- Everything else copied nearly identically
- Users were very trusting because it didn't ask for much personal info, linked to anti-phishing how-to, linked to the real BOW's Verisign certificate popup, linked to the real BOW's Chinese language version of the page
- Essentially, nobody thought a spoof site would go to this level of detail
- Fooled the participant with the highest level of security expertise
- Only two participants correctly identified it, one noticing the double "v", the other noticing a stale date

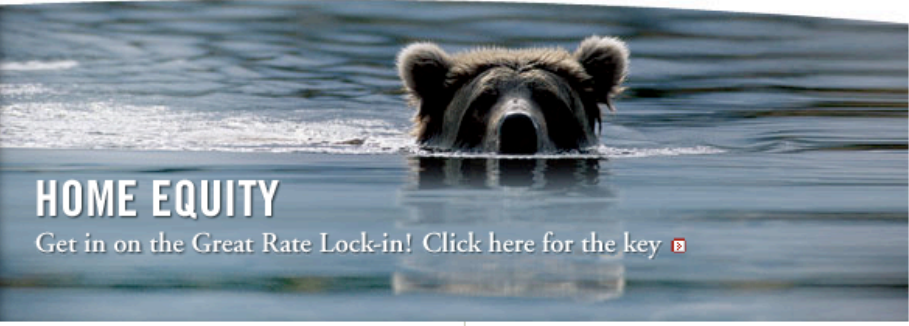


- » PERSONAL
- » SMALL BUSINESS
- » COMMERCIAL
- » ABOUT US

Online Banking

[Learn More](#) | [Enroll Online](#)
eTimeBanker® Sign In:
 User Name:
 Password:

[Forgot Password?](#)
Other Online Services:



HOME EQUITY
 Get in on the Great Rate Lock-in! [Click here for the key](#)

Locations

State:
 ZIP code:

CONSUMER ALERT!
 Tips on protecting yourself and how to report suspicious activities
[READ MORE »](#)

News Bulletin

June 14, 2005 | BancWest Corporation Announces Acquisition of Commercial Federal Corporation by Bank of the West
[More](#)



Personal Banking

Welcome to your community bank.
 First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

- [Checking](#)
- [Savings & CDs](#)
- [Debit & Credit Cards](#)
- [Online Banking](#)
- [Wealth & Trust](#)
- [Consumer Loans](#)
- [Private Banking](#)
- [More ...](#)

Tennis. Beach Games. Rodeo.

Join us for summer fun this week only!



Click on any logo to visit each official event website or [click here](#) to visit our sponsorships page that includes a broadcast schedule for the Classic.

Investments
 Retirement planning starts with an investment of about 15 minutes.

Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

- [Business Checking](#)
- [Cash Management](#)
- [Merchant Services](#)
- [Loans & Lines](#)
- [SBA Lending](#)
- [More...](#)

Commercial Banking

Your cornerstone of stability and growth.

Middle-market to multi-national, our corporate clients give us high marks for flexible financing, fast local decision-making, and a proactive style of client service. Let's talk business.

- [Commercial Lending](#)
- [Cash Management](#)
- [Capital Markets](#)
- [Equipment Leasing](#)
- [International Trade](#)
- [More...](#)



TaxDirect
 Pay your business taxes online - quickly and securely.

Results Compared to Hypotheses

- Lack of computer system knowledge led to vulnerability
- Experienced users tripped up with visual deception
- *New*: Lack of knowledge of web fraud
- *New*: Erroneous security knowledge

Conclusions

- Even in best scenario, with users expecting spoofs to be present, good fishing site can subvert 90% of users
- Trustworthiness indicators misunderstood and misused
- A new approach for website security is needed – cryptography cannot be the sole security measure
- Really need to think of new ways to help novices more easily identify fraudulent sites, both through improved measures and better training

Questions/Concerns?

- Mine: Why not a larger sample size?
- Yours...???