CSC 482/582: Computer Security

Usability and Psychology
Topics

1. Social Psychology
2. Social Engineering
3. Phishing
4. Marketing Psychology
5. CAPTCHA
6. Phreaking
7. Risk Assessment Heuristics
8. Usability
Psychology and Security

Psychology provides tools to study human behavior.

Helps us understand users
• How do users behave and why?
• Human-Computer Interaction (HCI)

And helps us to understand threats
• How to threats behave and why?
• Criminology
Asch Conformity Experiments

- Simple perceptual task
  - Student participant
  - 7 other participants were actors.
- Experiment actually focused on how the participant would react to the behavior of the actors.
  - First two trials, actors would give right answer.
  - Starting with 3rd trial, actors would give unanimous wrong answer to 12 of 18 total trials.
- 75% of participants gave at least one incorrect answer.
Milgram Experiments

- Series of social psychology experiments to measure willingness of participants to obey authority figures.
- 65% would obey the Experimenter, giving what they thought was a dangerous shock to the Learner.
Stanford Prison Experiment

- Psychological study of responses to captivity and its behavioral effects on authorities and inmates in prison.
- Discontinued after 6 days.
Strip Search Call Scam

- Series of calls to fast food restaurants in small towns
  - Caller identified self as a police detective
  - Claimed a female employee was a criminal
  - Requested manager to hold employee until he could arrive.
  - If early requests went well, requested strip search.
- Continued for 10 years until a 2004 incident in Mount Washington, KY led to arrest of David Stewart.
- Movie *Compliance (2012)* about KY incident.
Social Engineering

- Use a plausible story, or just bully the target
  - ‘What’s your PIN so I can cancel your card?’
- Exploits our social psychology
Social Engineering Techniques

Pretexting
- Creating an invented scenario to convince victim to divulge information or perform actions to help attacker.
- Ex: pretend to be sysadmin, co-worker, police, etc.

Phishing
- Lure victim to use fake login site to collect authentication info.

Baiting
- Send USB drive/CD with malware to victim or leave in location near business to be found and used.

Diversion Theft
- “Round the Corner Game”

Tailgating
- Follow legitimate user into restricted area.
Phishing is a criminal attack employing both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials.

### Statistical Highlights for 1st Quarter 2013

<table>
<thead>
<tr>
<th>Category</th>
<th>January</th>
<th>February</th>
<th>March</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unique phishing e-mail reports (campaigns) received by APWG</td>
<td>28,850</td>
<td>25,385</td>
<td>19,892</td>
</tr>
<tr>
<td>from consumers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of unique phishing websites detected</td>
<td>46,066</td>
<td>35,024</td>
<td>36,983</td>
</tr>
<tr>
<td>Number of brands targeted by phishing campaigns</td>
<td>402</td>
<td>348</td>
<td>405</td>
</tr>
<tr>
<td>Country hosting the most phishing websites</td>
<td>USA</td>
<td>USA</td>
<td>USA</td>
</tr>
<tr>
<td>Contain some form of target name in URL</td>
<td>50.03%</td>
<td>50.75%</td>
<td>55.89%</td>
</tr>
<tr>
<td>No hostname; just IP address</td>
<td>1.84%</td>
<td>1.92%</td>
<td>5.24%</td>
</tr>
<tr>
<td>Percentage of sites not using port 8</td>
<td>1.36%</td>
<td>2.33%</td>
<td>0.64%</td>
</tr>
</tbody>
</table>
Phishing is a Growing Attack
Phishing Targets Everyone

Most Targeted Industry Sectors 1st Quarter '13

- Payment Services, 45.48%
- Financial, 23.95%
- ISP, 8.52%
- Retail/Service, 9.84%
- Gaming, 5.66%
- Social Networking, 2.15%
- Government, 2.11%
- Auction, 1.84%
- Classifieds, 0.45%
Dear Sky Bank customer,

We recently reviewed your account and suspect that your Sky Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the Sky Financial network is our primary concern. Therefore, as a preventive measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your Sky Internet Banking account. In case you are not enrolled for Internet Banking, you will have to fill in all the required information, including your name and your account number.

2. Review your account history for any unauthorized withdrawals or deposits, and check your account profile to make sure no changes have been made. If any unauthorized activity has taken place on your account, report this to Sky Financial Group staff immediately.

To get started, please click the link below:

SIGN-ON

©2005 Sky Bank Financial Group. All rights reserved.
Phishing Site

Sky Online Banking Users - Microsoft Internet Explorer


Fraud Alert! Help Protect Your Accounts. Remember, always access Sky Online Banking by going to www.skyfi.com directly and not through links from other sites or sent in an e-mail message. NEVER click on a link in an e-mail message, open an attachment, or reply to any e-mail message that warns you that an account of yours will be closed unless you confirm your billing information or asks you to verify personal information to activate a feature. If you think your Sky Bank account information has been compromised, contact Sky at 1-866-SKY-BANK (1-866-759-2265). Report any suspicious activity to the FTC and send the actual e-mail message to use@ftc.gov. Sky does not contact clients via e-mail, phone or mail to request or verify security information about passwords or PINs. In addition, for your protection, when you call our financial center or the Sky Client Call Center, our representatives use special "know your caller" procedures to prevent unauthorized distribution of your personal account information. Find out more about how to protect yourself from identity theft. Do you need help signing on? Click here for instructions. If you need additional assistance, send e-mail to personal@skyfi.com or call our Client Service Center at 1-866-SKY-BANK (1-866-759-2265) Monday through Friday 7 a.m. to 7 p.m. or Saturday 8:30 a.m. to 1:00 p.m.

If you need to sign up for Personal Online Banking, you can apply for it by filling out and sending in this personal online banking application form.
Types of phishing URLs

- Misleading domain name
  - http://www.banckname.com/
  - http://www.bankname.com@www.example.com/
  - http://www.bankname.xtrasecuresite.com/

- Insecure end user
  - http://www.example.com/~user/www.bankname.com/

- Insecure machine
  - http://www.example.com/bankname/login/

- Internationalized domain names
  - paypal (Russian Cyrillic characters in a unicode font)
  - actual text is “raural”
  - paypal (Standard Latin characters in a unicode font)
Picture in Picture Attacks
Spear Phishing

- Spear-phishing is a phishing attack against a small set of specific targets.
- Uses victim personal information for authenticity:
  - Name
  - Phone number
  - Organization details
- Greater % of targets respond.
Phishing Site Lifecycle

**Hours 0-1**
- **Phisher:** Registers domain with Registrar
- **Phisher:** Creates phish site

**Hours 1-12**
- **Phisher:** Creates and sends phish email
- **Consumer:** Receives email
- **Anti-phishing service provider** like MarkMonitor or Brand Owner:
  - Identifies site, investigates, and initiates shut down procedures

**Days 3+**
- **Consumer:** Loses an average $1,244 in 2006
- **Phisher site disabled**
- **Anti-phishing service provider** like MarkMonitor or Brand Owner:
  - Disables site by contacting ISP, Registrar, or Site Owner
- **Law Enforcement:** Starts investigation (usually weeks later)
Phishing Countermeasures

- Block phishing emails
- Block phishing websites
  - Firefox and Chrome use Google’s blacklist
  - IE uses Microsoft’s blacklist
- Better user interfaces
- Educate users
Banks vs. Phishing

- Banks pay firms to take down phishing sites
  - Identify site
  - Identify ISP, registrar, or owner responsible for site
  - Send shutdown request to site
- Mule recruitment seems to be a serious bottleneck
First-rate, premium quality carrier
over 40 years of quality service

QUALITY, FAIRNESS, HONESTY and UNCOMPROMISING CUSTOMER SERVICE.

Since its establishment in 1959, Waller Truck Co., Inc. has centered its family-owned trucking business on: QUALITY, FAIRNESS, HONESTY and UNCOMPROMISING CUSTOMER SERVICE.

Because your product is your investment, we take shipping your product and protecting your investment seriously. Waller Truck Company’s well-maintained, market-responsive equipment, strong supply of quality drivers and dedication to service make meeting your delivery times a habit, and one that will continue. From every angle of quality, commitment and customer service, Waller Truck Company is serious about being a leader in the industry.

TRUCK DRIVERS
see what Waller has to offer you

EQUIPMENT SALE
buy equipment from Waller
1. Regional Sales Manager

Status: Part-time

Job description:
- Work as a member of a group, helping to enlarge a base of customers in countries all over the world and liaise with head office on a daily basis;
- Deliver high standards of customer service ensuring high delivery speed and quality of orders;
- Manage a part of a sales cycle – ensure fast remittance of payments through your bank account and then - through world wide Western Union system and calculate fees at each step;
- Create and maintain positive relationships with existing clients that result in new customers, lead to and maximise opportunities for expansions and renewals to enhance revenue stream.

Employees should be able to perform:
- Excellent spoken English & communication skills (oral and written).
- Professional approach on the phone conversations
- PC literate: Microsoft Outlook and Word as a minimum
- Proven ability to communicate effectively at all levels in a relaxed confident manner.
- Extroverted and outgoing, with a positive outlook.
- Significant attention to detail.
- Excellent organisational skills.
- Customer focused.
- Focused on own personal goals, integrating the achievement of company objectives.
- Ability to work unsupervised No previous sale or accounting experience is necessary, though it will be valued.

Your Personal situation must allow you to travel around your place 1-2 hours a day on company assignments( that would be particularly trips to the bank and Western Union branches)
Apply for this Position

WE OFFER:
- A base salary with generous commissions (10% out of each payment you've dealt with) and expenses.
- Flexible timetable – allows you to choose the most suitable time to deal with company assignments.
- Benefits, including Contributory Pension, Life Assurance, Private Medical Insurance, Birthday holiday Day and Childcare vouchers.

2. Warehouse supervisor

Status: full-time
Job description:
- Provide health and safety of all staff and visitors to the warehouse and goods in area;
- Make accounting for quality and storing of incoming goods;
- Make stock records of all stock in warehouse;
- Correct assembly of orders against shipping documents;
- Supervise cleanliness of the warehouse and production area;
- Monitor loading of vehicles to meet shipping dates;
- Inspect maintenance of all mechanical handling equipment within the Company.
- Supervise and manage all staff reporting to you.

Employees should be able to perform:
1 Knowledge of Warehouse Operations
2 Stock Control skills
3 Knowledge Warehouse IT Systems
4 Supervision of Staff
5 Professional approach on the phone and in face-to-face meetings.
6 PC literate: Microsoft Excel, Outlook & Word as a minimum.
Mule recruitment

- Proportion of spam devoted to recruitment shows that this is a significant bottleneck
- Aegis, Lux Capital, Sydney Car Centre, etc
  - mixture of real firms and invented ones
  - some “fast-flux” hosting involved
- Only the vigilantes are taking these down
  - impersonated are clueless and/or unmotivated
- Long-lived sites usually indexed by Google
Fraud and Phishing Patterns

- Fraudsters do everything that marketers do
- IT industry has abandoned manuals – people learn by doing, and marketers train them in unsafe behavior (click on links...)
- Bank approach is ‘blame and train’ – long known to not work in safety critical systems
- Their instructions ‘look for the lock’, ‘click on images not URLs’, ‘parse the URL’ are easily turned round, and discriminate against nongeeks
Marketing Psychology

- People make buying decisions with the emotions and rationalize afterwards
- Mostly we’re too busy to research each purchase – and in the ancestral evolutionary environment we had to make flight-or-fight decisions quickly
- The older parts of the brain kept us alive for millions of years before we became sentient
- We still use them more than we care to admit!
Marketing Psychology

- Mental shortcuts include quality = price and quality = scarcity
- Reciprocation can be used to draw people in
- Then get a commitment and follow through
- Social proof: like to do what others do
- People also like to defer to authority
- They want to deal with people they can relate to
Framing effects include ‘Was £8.99 now £6.99’ and the estate agent who shows you a crummy house first.

Take along an ugly friend on a double date ...

Typical phishing attack: user is fixated on task completion (e.g. finding why new payee on PayPal account)

Advance fee frauds take this to extreme lengths!

Risk salience is hugely dependent on context! E.g. CMU experiment on privacy
CAPTCHAs

Completely Automated Public Turing test to tell Computers and Humans Apart

Idea: stop automated digital attacks on account registration and similar applications by limiting access to interactive human users.
A Turing test is a test of a machine’s ability to exhibit intelligent behavior indistinguishable from that of a person.

A reverse Turing test reverses the roles of the machine and the person: a machine administers the test to see if input is coming from a human or a machine.
How CAPTCHAs Work

1. Generate a word or string of characters at random.
2. Generate an image containing a distorted rendering of the string.
3. Administer a test, requesting that the word in the image be typed in.
Problems with CAPTCHAs

- Unusable to visually impaired users.
  - Can use voice CAPTCHAs, as voice recognition of short words by an unknown speaker is a hard AI problem too.
- Newer graphical CAPTCHAs are hard for anyone
Defeating CAPTCHAs

1. Relay Attacks
   1. Re-use CAPTCHA on a site that you control, then use the solution when a person solves it for you.

2. Optical Character Recognition
   1. Remove background clutter.
   2. Segment image into pieces, each with a single letter.
   3. Identify the letter for each segment.

3. Attack CAPTCHA software.

4. Hire someone to solve it for you.
   1. Mechanical Turk crowdsourcing techniques.
Phone Phreaking

- Phone system under attack since 1960s!
  - Cap’n Crunch
- 1970s – systematic attacks on signaling
  - Blue boxes
- 1980s/90s – attacks on switching, configuration
  - Poulsen, Mitnick
Phone System Lessons

• It’s so like the history of Internet crime!
• Hacks invented for fun get used by crooks
• Vulnerabilities found at all levels
• A weak foundation, such as the phone company payment system, grows until it’s too big to change, then gets targeted
• Things take off once money extraction can be industrialized
• Then stakeholders dump risk and run for cover
## Psychology and Risk Assessment

<table>
<thead>
<tr>
<th>People exaggerate risks that are:</th>
<th>People downplay risks that are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectacular</td>
<td>Pedestrian</td>
</tr>
<tr>
<td>Rare</td>
<td>Common</td>
</tr>
<tr>
<td>Personified</td>
<td>Anonymous</td>
</tr>
<tr>
<td>Beyond their control, or externally imposed</td>
<td>More under their control, or taken willingly</td>
</tr>
<tr>
<td>Talked about</td>
<td>Not discussed</td>
</tr>
<tr>
<td>Intentional or man-made</td>
<td>Natural</td>
</tr>
<tr>
<td>Immediate</td>
<td>Long-term</td>
</tr>
<tr>
<td>Rapidly occurring</td>
<td>Evolving slowly over time</td>
</tr>
<tr>
<td>Affecting them personally</td>
<td>Affecting others</td>
</tr>
<tr>
<td>New and unfamiliar</td>
<td>Familiar</td>
</tr>
<tr>
<td>Uncertain</td>
<td></td>
</tr>
<tr>
<td>Directed against their children</td>
<td></td>
</tr>
<tr>
<td>Morally offensive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Associated with some ancillary benefit</td>
</tr>
<tr>
<td>Not like their current situation</td>
<td>Not like their current situation</td>
</tr>
</tbody>
</table>
Defining Usable Security

Security software is **usable** if the people who are expected to use it:

1. are reliably made aware of the security tasks they need to perform;

2. are able to figure out how to successfully perform those tasks;

3. don't make dangerous errors; and

4. are sufficiently comfortable with the interface to continue using it.
Usability Problems for Security

Unmotivated Users
- Security is usually a secondary goal.

Abstraction
- Security policies abstract, unintuitive to users.

Lack of Feedback
- State of security configuration complex.
- Little feedback: was that connection really encrypted?

Barn Door
- If information unprotected at one time, attacker may have already read or modified it.

Weakest Link
- Threat needs to only exploit one security weakness.
Why Johnny Can’t Encrypt

Usability evaluation of PGP 5.0

- Pretty Good Privacy
- Encrypts data
- Plugins for e-mail clients

Results of study of 12 users

- 3 users sent e-mail without encryption (2 of 3 realized)
- 7 users used public key instead of private key to encrypt
- Only 2 users could decrypt without problems
Key Points

1. Social engineering attacks are an effective means of attack for threats and cannot be stopped by technology alone.
   1. Phishing, baiting, pretexting, tailgating, diversion theft
2. Human risk assessment heuristics not effective against modern threats.
3. A CAPTCHA is a reverse Turing test based on hard AI problems to stop automated attacks.
4. Phishing attacks
   1. Picture-in-picture, spear-phishing, money mules.
References