Security User Studies Workshop
SOUPS 2006

July 12, 2006

Proposed user studies

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Spam mail acceptance study

2. Purpose of Study: *Please provide a concise statement of the background, nature and reasons for the proposed study. Use non-technical language that can be understood by non-scientist members of the panel.*

Despite the large amount of unsolicited email received by most Internet users on a daily basis, very little is known in the academic literature about what makes people likely or unlikely to respond to such mail. This study is designed to increase academic understanding of what factors make spam email more likely to be received, read, and responded to

3. Study Protocol: *Please provide a detailed description of your proposed study.*

We have collected the email addresses of approximately 30 million Internet users through the use of a web scraper. We wil email each of these users between 1 and 20 times each day with a variety of different email messages. The email messages will distinguish themselves using a variety of techniques:

* Some will have "From:" addresses that match the recepient, while others will have "From:" addresses that are from other email addresses that we have collected in the same domain as the user.

* Some email messages will be plain text, others will be HTML, others will include just an image, while others will have active content such as Flash or Java/JavaScript.

Some email messages will urge the user to click on an embedded link, arguing that they are in financial risk or that their computer is infected with a worm. Other email messages will include an attached program. Still others will have an 800-number that the user is instructed to call.

We will measure the response rate of users who click on the links, run the software, and telephone the 800-number.

Some of the email messages that contain an embedded executable will have software that turns on any firewire or USB cameras that are connected to the computer in question. A short (5 second) video segment will be sent to our Internet-attached computer. This is designed to allow us to determine who has clicked on the link.

Our software may collect additional personal information when it runs.

Some of our email will explain to the recipients that their name has been chosen to participate in an important scientific experiment. Other email messages will not mention the study. We will be investigating the impact of IRB-suggested disclosure on the study response rate.

Subjects

4. Estimated Number of Subjects:

30 million

5. Estimated Age of Subjects:

6-80

6. Criteria for inclusion/exclusion of subjects:

We were able to find the subject's email address on a web page.

We will be including children, cognitively impaired persons, non-English speakers, students, and all other populations for which the members have email addresses. They are being included because it is not feasable to exclude them.

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

Subjects will be sent an email message. Those that follow its instructions will have recruited themselves.

8. Compensation:

Compensation goes here

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

There is no known risk that can result from receiving an email and clicking on a link.

What procedures will be in place to prevent/minimize potential risks or discomfort:

Subjects are already receiving so much unsolicited email that the additional mail that they receive as part of this experiment will not be noticed.

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

Subjects will have a chance of winning an Apple i-Pod.

What potential benefits can society expect from the study?

Society will learn more about what factors cause email to be ignored or responded to.

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Risk Perception of Wireless Computing

2. Purpose of Study: *Please provide a concise statement of the background, nature and reasons for the proposed study. Use non-technical language that can be understood by non-scientist members of the panel.*
In the past several years, wireless internet usage, both in and away from the home, has dramatically risen in popularity. We are proposing a study to that investigates what people understand about wireless technology and its risks, and whether perceived risk and trustworthiness of particular wireless access points affect how people use them.

Existing research in online trust makes little distinction between trust associated with online vendors/website content and trust associated with infrastructure/connection to these resources. Several studies of online trust mention that some internet users may be concerned with trusting connections/infrastructure, but this issue is not the focus of the studies. As a result, there is a gap in the body of online trust research. Although we know quite a bit about factors leading to websites or vendors seeming trustworthy, we don't know much about what makes a wireless connection trustworthy, and many of the factors that are known to contribute to trust of vendors/content simply don't apply in the context of trusting a connection. Our study will help to fill this gap in the body of online trust research.

3. Study Protocol: *Please provide a detailed description of your proposed study.*
We would like to recruit frequent and occasional users of wireless internet to discuss their experiences and perceptions of risk with respect to wireless computing. Their participation will involve completion of two activities. The first activity is a questionnaire that asks for information about the participant and his/her experiences with computing and the internet (both wired and wireless). The second activity is a qualitative interview that asks about wireless internet usage and risks associated with wireless internet usage.

The interview will consist of five parts: a set of opening questions about wireless computing usage, a sketching exercise, a card sorting exercise, a set of questions about perceived risk, and completion of a survey asking about perceived risk in particular situations.

Opener
The interviewer will ask the following questions to learn about the participant's initial Wifi usage, current usage, and whether usage has changed over time:
1. When did you first start using wireless internet? Why?
2. How do you find wireless networks that you can use?
3. In what situations do you now use wireless internet? For what purpose do you use it? Do the things you do with wireless internet change based on where you are using it?
4. Do the things you do with wireless internet change based on what you know about the wireless network itself? (If needed, the interviewer can prompt by asking questions such as "How about who is running the network? How about what sort of wireless network it is? How about the name of the network?")
5. Have you ever had any problems when using wireless internet? What did you do about it?

Sketching Exercise
Next, the participants will explain what they understand about the technical functionality of wifi by completing a short sketching exercise. To complete this exercise, the participant should be instructed to draw a diagram of what he or she believes occurs in the time between typing http://www.google.com into a web browser and pressing "go" and the web page appearing (1) on a wired network, (2) on a wireless network, (3) on a computer-to-

computer network. Participants will be provided with a new sheet of paper for each sketch, and may refer to previous drawings for each portion of this exercise.

Card Sorting Exercise
A card sorting exercise will be used to find out what participants perceive are risks associated with wireless computing, and whether these risks affect their wifi usage. The participant will write risks associated with wireless internet connections on a set of index cards and note whether they apply to Wifi in public settings, private settings, or both. Then he or she will rank the risks by numbering the cards. The interviewer should ask questions as needed to clarify reasons for choices of risks/rankings. If participant lists security or privacy concerns in rankings, the interviewer should ask about steps he/she takes to protect self. Does the participant use firewalls, encryption, virus scanners, refrain from accessing sites about sensitive subjects, etc?

General Questions About Perceived Risk
These questions are intended to elicit answers about how the participant deals with risks associated with wireless computing. The interviewer should ask the following questions.
1. Have you ever connected to a wireless network without knowing who is managing it and/or why it is available for a person like you to use? (If yes, the interviewer should prompt to find out why participant used the connection, and whether activity was different than in a situation in which user knows more about the hotspot)
2. Do you ever worry about other people accessing your files or data when you are using a wireless internet connection?
3. Do you ever worry about other people seeing what you are doing without your permission when you are using a wireless internet connection?
4. Have you ever found a wireless internet connection you wouldn't use? (If no, the interviewer should ask "Is there anything you wouldn't use a wireless internet connection – public or private - for?")
5. In general, what does the name of a wireless access point/hotspot tell you about it?
6. What does it mean to you if a wireless connection is "security-enabled"? "Unsecured"?

Perceived risk in particular situations
In this activity, we would like to learn how participants perceive and deal with risks in particular scenarios. The participants will be given two Likert-scale surveys to fill out during the interview. The first survey asks about how likely a participant would be to perform several different activities (e.g. purchasing an item online, browsing heath information, chatting on instant messenger) using a device he or she owns on the following types of connections: a wired connection, an unsecured wireless network, a security-enabled wireless network, an unsecured computer-to computer network, and a security-enabled computer-to-computer network. The second survey asks how likely a participant would be to perform the same set of activities on a device he or she does not own on the same list of connections as in the first survey. After the participant completes the surveys, the interviewer should prompt to find out why the participant made particular choices.

Subjects

4. Estimated Number of Subjects:

5. Estimated Age of Subjects:
6-80

6. Criteria for inclusion/exclusion of subjects:

Frequent and occasional users of wireless internet

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

8. Compensation:

Compensation goes here

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

What procedures will be in place to prevent/minimize potential risks or discomfort:

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

What potential benefits can society expect from the study?

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Biometric Acceptance Based on Context of Use

2. Purpose of Study: *Please provide a concise statement of the background, nature and reasons for the proposed study. Use non-technical language that can be understood by non-scientist members of the panel.*

Biometric systems have increasingly been deployed over the past years with mixed results on their effectiveness. General public acceptance of biometrics, while increasing in some areas, is still slow. Research has shown that the usability and acceptance of biometric security services is affected by several factors, one of which we believe is the context of use. This exploratory study is conducted as an experiment that will manipulate the benefit and privacy dimensions within different contexts, and looks at the subjective differences. An experimental study has been designed to collect data using not only quantitative methods, but also qualitative procedures in an effort to get a deeper understanding for user perceptions. The expected results will show that the context that the biometric device is placed will have an impact on user acceptance.

The hypothesis for the research: The usability and acceptance of biometric security services will be affected by the context of use. Two important contextual factors will be perceived benefit to the user and perceived privacy risks. Application contexts with obvious, apparent benefits will lead to greater perceptions of usability and higher acceptance opinions than contexts where there are little obvious benefits. Also, application contexts that are perceived to have high privacy risks will lead to lower opinions about usability and acceptance than contexts where there are minimal privacy risks.

This research we will focus on privacy perceptions when using the fingerprint scan biometric device. Our goal is to gather data on the user's perception of fingerprint biometrics for authentication within different contexts, focusing on the users' perspectives when deciding on the tradeoffs between perceived benefits and perceived privacy risk.

3. Study Protocol: *Please provide a detailed description of your proposed study.*

The study will be conducted as a lab experiment. This study is exploratory in nature so a mixed approach of qualitative and quantitative methods will be used in an effort to get more insight into user's perceptions. There are 4 separate tasks that the participants will be asked to complete. After each task, a survey will be completed interactively; whereby the participants will be observed as they complete the survey, and their responses orally discussed and recorded. The survey responses will be analyzed using quantitative methods, while the verbal responses will also be coded and reviewed. We hope to use the responses to the interviews to get a more in-depth understanding of the user's perspectives and perceptions to the questions asked in the survey. It would also be interesting to see how their verbal responses correlate with their

survey responses.

Subjects

4. Estimated Number of Subjects:

30

5. Estimated Age of Subjects:

18-80

6. Criteria for inclusion/exclusion of subjects:

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

8. Compensation:

Candy Bar, refreshment

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

There are no physical risks. A participant may feel uncomfortable giving their biometric. We will address that right at the very beginning of the experiment,

What procedures will be in place to prevent/minimize potential risks or discomfort:

We provide an explanation of what the scanner is actually storing, and can unplug the device

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

They may be familiarized and get an understanding of the fingerprint biometric scanner

What potential benefits can society expect from the study?

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Verified Password for a Candybar

2. Purpose of Study: *Please provide a concise statement of the background, nature and reasons for the proposed study. Use non-technical language that can be understood by non-scientist members of the panel.*

Although there have been several studies in which computer users were offered a candy bar or other enticements for revealing their passwords, none of these studies verified that the revealed passwords were correct. Likewise, none of these studies clarified precisely which kind of password was being revealed.

The purpose of this study is to determine if office workers really will reveal their passwords for a token payment, such as a candy bar, and the quantify specifically which type of passwords they will provide. We also wish to examine any bias that may result from the gender of the experimenter.

3. Study Protocol: *Please provide a detailed description of your proposed study.*

Protocol goes here.

We will set up a table at Boston's South Station. On that table will be a computer equipped with wireless Internet access, a bowl of chocolate bars, and a copy of our IRB approval.

As commuters arrive during the morning rush hour, an experimenter will approach individuals and ask if they would like to participate in a 3 minute experiment. The experiment, they are told, is that they have to reveal a password. In return, they will get a chocolate bar. (Subjects that are allergic to chocolate will be offered a $3 Starbucks gift card as an alternative.)

Commuters will be given the choice of revealing their password or not. All revealed passwords will be demonstrated on our wireless laptop to prove that they work.

We will divide our subjects into two groups:

Group 1 - These subjects will be told that their password will be recorded by the computer. (The password will not actually be recorded.)

Group 2 - These subjects will be told that their password will NOT be recorded by the computer. (The password will not be recorded.)

After the password is typed, we will ask the subject if they provided a password for a personal, home account, or for a work account.

- If the subject provides a password for a home account, the subject will be told that they

need to provide the password for a WORK account in order to receive the candy bar.

- If the subject provides a password for a work account, the subject will be told that they need to provide the password for a HOME account in order to receive the candy bar.

The subject will then be given an opportunity to provide the other password.

We will:

- Take notes of everything the subject says
- Note the gender and age of the subjects.
- Note the gender and age of the person who approaches the subject. (Prior work by Smith detected a significant gender bias, in that female experimenters were far more likely to elicit valid passwords from male subjects than other gender combinations.)

Some subjects will be told that their username and password will be recorded by the computer, even though this is not the case.

Subjects

4. Estimated Number of Subjects:

100

5. Estimated Age of Subjects:

18-65

6. Criteria for inclusion/exclusion of subjects:

We will approach subjects in the train station

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

Recruitment goes here

8. Compensation:

Subjects will receive a candy bar and/or a $3 Starbucks gift card. The subjects may also learn about computer security.

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

Subjects may feel guilty for putting the security of their home computers or workplaces at risk.

What procedures will be in place to prevent/minimize potential risks or discomfort:

Subjects will be shown our IRB approval.

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

Benefits to the subject

What potential benefits can society expect from the study?

Society needs to understand how vulnerable people are to giving up their passwords through this kind of social engineering.

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Field Study of Security Administrators

2. Purpose of Study: *Please provide a concise statement of the background, nature and reasons for the proposed study. Use non-technical language that can be understood by non-scientist members of the panel.*
The overall goal of this field study is to investigate security administrators in order to understand and model their tasks as well as the effectiveness and usability of the tools they currently use to perform these tasks. Specific objectives are: 1) provide inventories of a) security administration errors, b) constraints and limitations manifest in the human, organizational and technological dimensions, and c) technologies; 2) provide rich data about the security administration task space.

3. Study Protocol: *Please provide a detailed description of your proposed study.*
We plan to conduct semi-structured, audio-recorded interviews of all the qualified subjects who chose to participate in the study. We expect an interview to take anywhere between one and two hours. A semi-structured interview will allow subjects to tell stories that provide information beyond the current situation or time-frame. The interviewer will have the opportunity to inquire about a wide range of aspects of security administration task, from minute routine details to long-term goals.

Job
• Please explain the general nature of your work from your point of view.

Communication
• What kind of people do you talk with during the course of your work? How do you talk with them— telephone, meeting, email, instant messaging.
• How does the information exchanged relate to your work?
• Who understands what you do?
• Under what circumstances do you have to explain your work?
• When do you feel like you have to translate something into your own language in order to do it?
• How does your organization support your responsibilities?
• How do you know whether or not people have realistic expectations of you?
• Under what circumstances are you asked to do things that you feel don't fit with your true responsibilities?
• Please describe a time when you felt like throwing up your hands and exclaiming Ok, have it your own way.
• Please describe which of your activities negatively affect other people.
• Please tell of other people's activities that negatively affect you.
• Please tell of times when someone was either unhappy or happy with your decisions.

Tasks
• In the pre-interview questionnaire, you indicated that you usually do these kinds of tasks [have list of tasks from pre-interview questionnaire]. Please talk about these tasks.
• How do they arise?
• What does it take to do them?
• What examples come to mind?
• Who or what do you consult when you need to know something? Under what circumstances does this happen?
• Which of your tasks do you do first, next, etc.? Please explain why?
• Please give an example of a having to put something off in order to do something more urgent. Under what circumstances does this happen?

Errors
• Please tell of a time when a situation went from bad to worse because of misunderstanding.
• Which errors do you find it is easier to make than others?
• How do you find out that you have made an error?
• Which kind of errors are more serious?
• Please tell of a time when you succeed at something, but in retrospect would have done it much differently.
• With respect to your responsibilities, please tell of a time when someone enacted policy that you would consider to be a strategic error.

Tools
• Under what circumstances do you feel that you have to keep too many things in mind?
• Under what circumstances is it painful to find something that you know is there?
• Under what circumstances do things seem tedious?
• Under what circumstances do you feel that it takes too much effort or time to get something done?
• When have you amazed yourself with your ability?
• Under what circumstances do you have to patch different tools together in order to get the needed task to be done?
• Which of your tools would you describe as flexible or inflexible?
• Which of your tools take more effort to learn and handle than others? Are they worth the effort?
• If you had a magic button, what would it do?
• Which of your skills with one set of tools can be transferred to another set?
• If money was no object, how would you change your tools? Why?
• Which tools do you like/dislike? Why?
• Which tools have been bought but are not used?
• Which tools have been eventually discarded? Why?
• Which tools have been replaced with other tools?
• Which tools have been upgraded? Why?
• Which tools do you wish for? Why?

Subjects

4. Estimated Number of Subjects:

5. Estimated Age of Subjects:

6. Criteria for inclusion/exclusion of subjects:

A pre-interview questionnaire will allow us to determine the suitability of the respondents for the study (i.e., their involvement in security administration activities) and give us the opportunity to develop individualized interview questions about tool use, communication, and task prioritization. It will also allow us to derive demographic information about the study subjects, such as education, seniority, who they work with, common tools and common tasks.

The questionnaire will be delivered by plain text e-mail, and interested subjects will respond by replying with the completed answers. We want to provide the simple and convenient interface of e-mail for responding to the questionnaire because we expect the potential subjects to be multi-tasking and unable to devote much time or attention to a questionnaire.

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

To recruit subjects for the study, we will contact interested management of IT departments of commercial organizations. The management will provide us with the names and email addresses of potential subjects. We will solicit participation of the subjects by contacting them over e-mail. Our first contact e-mail messages will contain a

brief description of the project and its goals, a statement of what their involvement would take, and an invitation for them to participate. Because of the security-related nature of this research, we will need to reassure respondents that their organizations are supportive of the study, while not requiring them to participate if they do not want to. Interested subjects will receive the pre-interview questionnaire.

8. Compensation:

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

What procedures will be in place to prevent/minimize potential risks or discomfort:

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

What potential benefits can society expect from the study?

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Trust Fall: Experimenting with Security Support

2. Purpose of Study: *Please provide a concise statement of the background, nature and reasons for the proposed study. Use non-technical language that can be understood by non-scientist members of the panel.*
This proposal describes a model for an experiment to test the efficacy of organizational support for security at the desktop end-user level. Rather than analyze the ability of end users to understand and respond to security threat, the Trust Fall model looks at the ability of the organization to respond to security problems, support end users, and build relationships with between IT personnel and end users. These relationships form the core of trust, and thus are leading indicators of the organization's ability to respond to certain types of threats.

The core of the Trust Fall model is to introduce a controlled security failure into an organization and carefully monitor and analyze the impact. Much as a honeynet can show how network vulnerabilities, a Trust Fall can show organizational vulnerabilities.

3. Study Protocol: *Please provide a detailed description of your proposed study.*
The first step in implementing a Trust Fall is to develop the security failure. For obvious reasons, introducing a viable threat, such as a real virus or worm, is inadvisable. As when medical doctors inoculate patients with a modified and non-dangerous virus, the Trust Fall requires a security exploit that can simultaneously trigger processes without exposing the organization to any real risk.

As a result, the Trust Fall model recommends a simpler approach: faking it. The end user has to be a confederate, in any case, so a simulated security lapse doesn't compromise the study. The easiest way to simulate is to rename a critical OS file (this may require booting of removable media). Before this is done, all files should be copied or moved to alternate media, because once the process starts, all hell may break loose.

Once the system has been properly corrupted, a call should be placed to the help desk or IT staff responsible. This may not be possible. Many IT groups have attempted to anonymize the support process by requiring that requests made online. This is, of course, the most preposterous approach. In at least some instances, the user won't be able to communicate via computer. However, assuming that the user can contact help desk, he should attempt to prime the support staff to assume a security problem. This can be done by stating that, for example, the virus scanner gave a warning before the computer crashed.

During a call or face-to-face interaction, the user should try a number of activities to investigate processes, IT staff knowledge, and other relevant parameters. These include, but are not limited to: admitting to reasonable but risky activities, such as downloading and running software, asking about how frequently to update virus scanning profiles, and asking about addition steps to secure systems. In this process, the user should look at how the support staff respond. Are they, in fact, supportive? Are they critical, do they blame the user? If they investigate potential sources for the problem, are they doing so to better understand the situation, or to be critical?

In addition, technical expertise can be measured. Does the support staff choose the optimal resolution path? Do they rely on the end user diagnosis (bad idea; many popups and websites tell users they have viruses)? Are they following organizational practices, industry best practices, or gut instinct? What are the differences between expertise of different staff members? Finally, how does the support staff make use of the interaction? Do they use it as an opportunity to help the user better understand security? Do they use it as an opportunity to help the user understand the IT support staff role? Would their demeanor, approach, and expertise serve to build trust on the part of the user?

Subjects

4. Estimated Number of Subjects:

IT support staff for larger corporations can number into the hundreds, or can be quite small.

5. Estimated Age of Subjects:

21-65

6. Criteria for inclusion/exclusion of subjects:

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

8. Compensation:

IT support staff are already compensated, and, as the Trust Fall will take place *in situ*, there is no need for additional compensation. As for the penalty or reward of the experience, one might use the cliché, "As ye sow, so shall ye reap."

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

The confederates risk being seen as abusing IT support resources, and the IT staff will be put into an emergency situation, which might cause stress, but a level of stress normal to the job.

What procedures will be in place to prevent/minimize potential risks or discomfort:

Ultimately, we can't minimize these risks. They exist and will persist. However, the risks are identical to what *will happen* in the course of normal business.

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

IT staff are not necessarily given opportunities to develop and display their skills, and if they are properly trained, with the correct approach, they could end up raising the level of esteem that IT support holds within the organization.

What potential benefits can society expect from the study?

We need to set the expectation that IT support staff have emergency responsibilities, in addition to daily responsibilities. The measure of success of an IT organization must be based upon both emergency action and daily action. The Trust Fall is a measure of IT response to emergency situations. Much as firefighters, police, and military regularly train for emergency situations, we need to train out IT staff using the same model. Without this training, the organization remains largely at risk.

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Anti-PhAshing

2. Purpose of Study:

PhAshing [fæʃing] refers to the attack of faked application through web browsers. The approach of counter measures against PhAshing is Anti-PhAshing.

Phishers are always trying their best to make the faked web pages look and behave as similar as possible to the real web pages. As the web browsers are adding more and more features (Java Script, ActiveX, Java Applet, Macromedia Flash, etc.), plug-ins (Adobe Acrobat, Google Toolbar, MSN Toolbar, OICQ, etc.), these features and applications are making web browsers "too" powerful that their UI is no just limited to the client windows in web browsers any more. Hence local applications, including the anti-phishing applications can be faked. A video at http://www.mit.edu/~ayf/my_free_sw/activeXAttack.zip demonstrates how ActiveX can take control the entire computer screen.

In this investigation, we use Web Wallet (an anti-phishing sidebar, www.mit.edu/~minwu) as an example to propose improved UI designs. We plan to use the following counter measures in the user study.

Control Study:
We provide control study UI, as shown in Figure 1, to make the other UI *anti-phAshing* improvements comparable. The difference from original *Web Wallet* design is that we use isolated window rather than embedding it into IE.

Application Trace:
We want to redesign a visual indicator, *Application Trace*. To testify one visual area is real, we have to set somewhere in the screen that cannot be faked. We tried to put the indicator as an icon in taskbar. However we found it is not secure, because the taskbar can be faked. Hence, we propose to put the visual indicator at a fixed physical area on the computer screen, e.g., at one of the four corners/sides of the screen, as shown in Figure 2.

Genuine Skin:
Genuine Skin is a method that can mitigate the difficulty of automatic *PhAshing* detection. There are several guidelines to design *Genuine Skin*, (a) *Genuine Skin Patter* is like trade mark, it is identical for a certain company, and a series of products of this company can use the same *Genuine Skin*. We consider it as illegal to use the images identical or similar to the *Genuine Skin* belongs to one company without authentication. (b) There's one *Anti-PhAshing* engine running in the client side to detect similar patterns to the *Genuine Skin Pattern* which are not in the known positions. (c) The design of *Genuine Skin Patterns* should be both easily recognizable by both human eyes and computers. We need to train the *Anti-PhAshing* engine to simulate the average human classification curve, such that we can reduce the numbers of both false positive and false negative. Good design of *Genuine Skin* can help reduce the false cases. Figure 3 shows two examples of *Genuine Skin* pattern designs for *Web Wallet*. (d) The suspected area will be circled and alert will given out if found, as shown in Figure 4. If the faked *Web Wallet* doesn't have *Genuine Skin*, then users will not tend to believe it is real, as shown in Figure 5.

Merged Approach:
The Anti-PhAshing task is difficult and there's no single tool can prevent users from PhAshing attacks at 100%. We have a hypothesis that if we use more anti-phishing techniques, we can gain more security. Hence, we would like to integrate Application Trace and Genuine Skin to carry out one user study to learn the effectiveness, as shown in Figure 6.

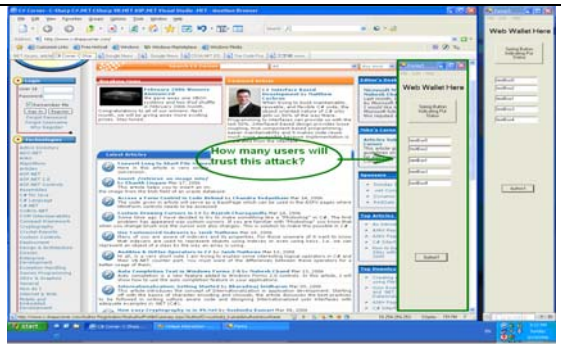

Figure 1 The Control Study UI

Figure 2 Application Trace Prototype

(a) Example 1

(b) Example 2

Figure 3 Genuine Skin Patter Examples

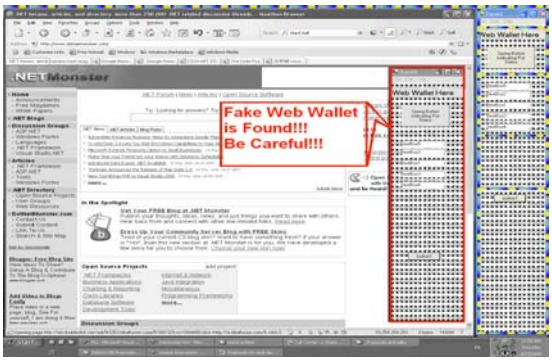

Figure 4 Anti-PhAshing engine found suspected pattern and gives out alert.

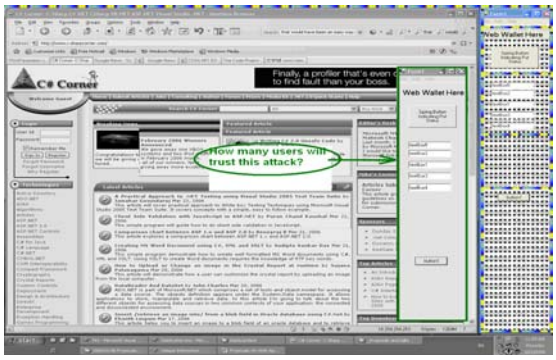

Figure 5 Users can easily recognize the faked Web Wallet

Figure 6 Prototype for merged anti-phAshing approach

3. Study Protocol:

We will recruit 4 groups of users. Each group contains 10 users to test one of the four types of methods (Control Study, Application Trace, Genuine Skin, and Merged Approach). We will design 10 "yes/no" questions for each user to answer whether the currently given Web Wallet is trustable. For each group, we will design 3 or 4 phishing attacks.

Subjects

4. Estimated Number of Subjects:

40 (10 for each method)

5. Estimated Age of Subjects:

6-80

6. Criteria for inclusion/exclusion of subjects:

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

8. Compensation:

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

What procedures will be in place to prevent/minimize potential risks or discomfort:

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

What potential benefits can society expect from the study?

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Autorun.info social engineering with CDROMs and USB tokens

2. Purpose of Study: *Please provide a concise statement of the background, nature and reasons for the proposed study. Use non-technical language that can be understood by non-scientist members of the panel.*

We wish to quantify the risk that the Microsoft "autorun" system poses to normal office workers, and to quantify how likely office workers are to trust media that they find in their environments.

3. Study Protocol: *Please provide a detailed description of your proposed study.*

We will distribute CDROMs and USB memory sticks at coffee shops. The devices will have a variety of different kinds of labels. Some will say "fun games" while others will say "paper" or even be blank. All of the devices will contain a program that automatically runs when it is inserted into a Windows or Macintosh-based computer. The program will send a message back to our server containing the following information:

* The kind of computer on which it is running
* Whether or not it is possible for the program to obtain administrative privileges.
* The number of Microsoft Word and Excel files that the program has access to.
* The amount of email that the program has access to.

The program will not actually compromise any of the personal information on the computer on which it is run.

After the program runs, it will cause a web browser to open that will display a page from our web server about good computer security practices.

Subjects

4. Estimated Number of Subjects:

100-1000

5. Estimated Age of Subjects:

6-90

6. Criteria for inclusion/exclusion of subjects:

We consider users of Microsoft Windows and Apple's MacOS to be a vulnerable population because they are running computer systems that, by default, automatically run programs on CDROMs and USB memory sticks that are inserted in the computers. We are specifically including these users in our study to determine how vulnerable this population actually is.

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

Subjects recruit themselves by picking up the CDROMs and USB sticks.

8. Compensation:

none

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

Subjects may be disturbed to find out how vulenrable they actually are.
Also, there is a chance of a bug in our software which might damage the user's computer.

There will be no informed consent. Subjects will not be told that they are in a study, because this would damage the study's external validity.

What procedures will be in place to prevent/minimize potential risks or discomfort:

We will test our software to minimize the chance of a bug causing data destruction.

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

Subjects may learn how vulnerable they actually are.

What potential benefits can society expect from the study?