PSYCH 499Y Honors Proposal
Student Deadline: August 15
Faculty Deadline: September 10

Statement of Purpose: What do you intend to discover or create during your Honors Thesis or Project experience?

According to a 2017 report by InfoSecurity (1), phishing attacks, or attacks in which a hacker poses as a trusted source to steal confidential user information, account for 95% of all successful cyber attacks worldwide. Phishing scams are successful because a user does not realize the website they are on is malicious. The absence of realization is partly due to a lack of paying attention, but also because of specific components of a site that do not sufficiently prove legitimacy. Even though phishing is a vast topic, there are two types of scams I will focus on within it, spoof websites and phishing emails.

A spoof website uses deceptive designs to imitate legitimate companies or organizations. By appearing to be a trusted source, the website fraudulently collects sensitive information from users. Some spoofed sites are so sophisticated that their layout appears almost identical to the trusted source they aim to imitate (2). At a glance, these websites often seem to be real, and it is easy for unsuspecting users to become victims of these scams. However, the surest way for someone to see if a link is legitimate or not is to check if the website URLs match the offered content. The reason URLs provide such an indicator is because every website has a unique domain (website name) and unique URLs (an address for a page on the internet) that redirect back to it. For example, if you click a URL that redirects to “https://mail.google.com,” “google.com" represents the domain name associated with all Google pages. Any legitimate organization or person must purchase a domain name, and therefore, spoofed websites that aim to imitate a trusted site cannot blatantly use their domain name. Therefore, a lot of spoofed website links usually contain more random text, but some smart hackers use domains that are very similar to the legitimate entity. For example, a familiar spoof for Microsoft (@microsoft) is (@rnicrosoft), as scammers take advantage of the small font size and style to make “rn” look like the “m.”

Google Chrome and similar modern browsers contain a built-in indicator that checks the security of a website. If a site is secure, Google features a tiny green lock and the word “Secure” in green text in the left-most corner of the browser. For websites that are not secure, the indicator displays a red caution icon and “Not Secure” in red text in the browser. In comparison to the overall website content, the security indicator has a small font and icon, resulting in the website content overpowering it.

Email spoofing is another popular method by which scammers obtain sensitive information from users. These emails are structured to mimic a legitimate entity by appearing to be sent by a trusted source and containing design elements and language that the trusted source would use. Additionally, these emails feature links in the email body that appear to be

legitimate but may redirect to a spoofed website. Unlike browsers, emails provide no sign of whether there is any danger in a particular link, and the user has to know how to classify the URL as dangerous. These emails usually feature website URLs in a hyperlink format. Traditionally, a hyperlink is an example of a mouseover (3), which is an element that gets activated when a user moves or “hovers” their mouse pointer over the element’s trigger area. Usually, the trigger area is some underlined text colored either blue or black, and a user can carefully hover over the text with their mouse to uncover the destination of the URL. When they do this, a tiny popup appears containing the full URL. This popup is not presented in an engaging enough manner to prevent accidental clicking, especially if a user is in a hurry. Constrained to a tiny box, the URLs long string of characters may cause a user to overlook small details within it.

Because interfaces do not present website URLs in a way that captures attention in time, people accidentally click on such links or fail to notice warning signs and become victims of phishing attacks. Through my thesis, I want to create proactive web components that warn the user and prevent such attacks before they even happen, and I want to use principles from visual and cognitive psychology research as the basis for creating these components. Cognitive psychology is the study of mental processes such as attention, perception, problem-solving, and more. This field provides insight into how users make decisions, prioritize information, or learn skills. Additionally, visual psychology research focuses on how the eyes and brain process information and drive interactions with the outside world. When using a web or mobile interface, humans rely on their vision to form judgments, process information and allocate attention to objects. Psychology lends an overall deeper insight on how humans interact and perceive information on an interface, and having this solid background can allow me to create these components to be in line with a user’s typical behavior.

I intend for these components to serve as an extension or enhancement of the browser or email service's backend functionality of detecting whether a site is illegitimate or not. I do not intend to change any of the backend algorithms that decide whether a website or email interface is secure or not. I want my implemented features to improve the design and presentation of URLs within a web browser or an email - this can be in regards to size, color, and many more aspects. Despite existing indicators, at this stage, human users are still going to be the best at validating whether a URL is secure, so by presenting the URL in a more attention-grabbing way, this offers a more proactive indicator of the redirected website's legitimacy for a user.

1. https://www.infosecurity-magazine.com/news/phishing-remains-top-attack-vector/
2. http://www.phishing.org/phishing-and-spoofing
3. https://www.techopedia.com/definition/2842/mouseover

2. Key Readings:

- *Designing with the Mind in Mind* by Jeff Johnson: This book is an excellent resource that goes in-depth on general visual psychology/cognition research and applies it to standard website design
- *What Attributes Guide the Deployment of Visual Attention and How Do They Do It?* Wolfe Horowitz (2004): This provides a general overview of visual cognition principles
- *Don't Make me Think* by Steve Krug -Has some insights on visual cognition, but they are mostly high level. More focus on actual website design, color, style elements, and conducting user research
- *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails* by Christopher Hadnagy and Michele Fincher: More focus on phishing emails, but a good overall resource for phishing as a wide topic
- Rensink, Ronald A. (2000) *When Good Observers Go Bad: Change Blindness, Inattentional Blindness, and Visual Experience.* [Journal (On-line/Unpaginated)]

I am also looking into Human Factors/Human-Computer Interaction and Applied Cognitive Psychology journals to find more information on using psychology to aid in interface design or similar applications.

3. Communication
    - How often will you meet with your primary Committee Chair?
        - Weekly 1-hour meetings/check-ins to discuss readings, insights gained, and the process of designing the experiment
        - 1.5-hour general lab meetings (attended by everyone in the Visual Cognition & Attention lab) to give status updates on research work
    - What are your Committee Chair's expectations of such meetings?
        - I complete all my assignments and come prepared to each meeting with insightful discussion points

4. Specialized Training

- CITI Training - will complete in August 2018 (before Fall semester)
- Psych Department Ethical Training - September 7, 2018

- Relevant Visual Cognition & Attention lab training (computers/technology/protocols) - throughout Fall 2018 semester

5. Methods

With my project, I want to create features that serve as an extension or enhancement of the browser's backend functionality of detecting whether a site is bad or not. In regards to phishing emails, I aim to change the presentation of hyperlinks within the email to be more attention-grabbing or proactive in nature.

Through the literature review, here are some areas I wish to study:

- The nature of phishing attacks: who gets targeted, how victims respond, attacker method, and more to provide context on why they are so effective. For the browser URL redesign, I will look into the measures current popular browsers (Chrome, Safari, Firefox) take to warn a user about website security and figure out areas of improvement. For emails, I will research on whether email anti-phishing warning indicators are in existence, and if they do exist, how effective are they? If none exist, I could propose design changes to the hyperlink's display.
- Past research in interface design and visual cognition and compile principles that justify my changes in the display of web pages and emails. I have already started gathering some principles, but I aim to get more detailed and relevant principles after completing the literature review:

Here are some principles that show how users interact with a web interface.

- Humans have a central-viewing bias when it comes to viewing screens
- Inattentional blindness: Because humans navigate a website based on a specific goal they have in mind, less prominent elements become overlooked. Usually, the URL is not the central aspect the user is trying to find and gets ignored.
- Scanning: According to Steve Krug in Don't Make Me Think, one of the most critical facts about web users is that they scan for the most relevant elements rather than read all the information.

These principles highlight that from the start, humans tend to not focus on the URL of a website. Thus, some principles below may lend some insight into how to redesign the browser to draw attention towards it:

- Exogenous orienting: A sudden change/movement in the periphery redirects attention towards it.

- Gestalt Similarity Principle: Items that look similar are perceived to belong together, but they also may be more easily confused with each other. It is hard to find distinctions between items with visually similar colors, sizes, or shapes. So, the eyes are more drawn to contrasting elements.

A significant component of my literature review will be dedicated to identifying principles like the above mentioned and reviewing existing research to learn more about these specific topics.

As for the experiment, I will create poorly designed web pages and emails that simulate phishing attacks, as well as well-designed web pages that incorporate the changes I have proposed. I will assign participants a basic task depending on the type of interface and enforce a certain time limit that emulates how much time a person would spend on the task. During testing, I will mix both the bad and good interfaces to avoid a participant from relearning or remembering a specific task. I will measure the effectiveness of the changes by recording the number of times participants are phished for both the poorly designed and improved interfaces. At the end of the experiment, I also will provide a survey that would ask phished participants what they wish would stand out more or what would have helped them prevent the attack.

6. Expected Timeline

September 15th: Write a summary on the origin and nature of both web and email phishing attacks

By October 10th: Identify the second member of the thesis committee

Withdrawal Period assignment (October 30): Draft of the section that will describe the visual psychology principles and their application in website/interface design

I also plan to have a list of interface changes that I wish to implement

November 1st: Completion of literature review & begin work on the 499T proposal

December 10th: Online submission of 499T/P Proposal