

# Research statement

Ponnurangam Kumaraguru (PK)  
School of Computer Science  
Carnegie Mellon University  
ponguru@cs.cmu.edu

With the rise of the Internet as a major mode for economic transactions and communication, online trust, and cyber crimes have increasingly become an important area of study in computer science, public policy and business. Today, individuals often do not know whether to trust an online merchant with their personal information or whether the emails they receive come from legitimate entities. Because of the increasing sophistication and volume of cyber attacks, Internet users are making incorrect decisions that cause significant economic damage to themselves and enterprises. As a result, developing technologies that help users make better online trust decisions has become important.

To develop usable and secure systems, I conduct research at the intersection of computer security and human computer interaction. Primarily, I focus on developing technologies and insights that help users to protect themselves from security attacks and thereby improve their ability to make online trust decisions.

## Research Background

### *PhishGuru*

I am currently involved in a project called Supporting Trust Decisions. This project aims to develop and test tools such as new email applications and training modules to improve trust decisions that will help protect Internet users against phishing attacks. Phishing scams con victims with legitimate looking emails and websites to steal bank account information, passwords, and other confidential information. I focus on developing theory and tools to educate users about phishing and improve their decision-making. Research shows that in 2007, 3.6 million adults lost \$3.2 billion in phishing attacks. Developing countermeasures for phishing is a challenging problem because victims help attackers by giving away their credentials. It is also difficult to detect phishing websites and emails because they often look legitimate. Using literature and my experience, I identified a number of challenges for end-user security education in general and anti-phishing education in particular: users are not motivated to learn about security; for most users, security is a secondary task; it is difficult to teach people to identify security threats without also increasing their tendency to misjudge non-threats as threats. Keeping these challenges in mind, I developed an email-based anti-phishing education system called PhishGuru. I am the lead developer of the PhishGuru, a system in which training messages are designed to look like phishing messages. When users “fall” for our training messages, PhishGuru takes advantage of the “teachable moment” and immediately teaches users how to avoid falling for real scams in the future. My studies demonstrate that PhishGuru effectively teaches people what cues to look for in order to distinguish scams from legitimate emails. I applied insights from learning science in the design and evaluation of PhishGuru.

Our previous user studies in the laboratory and in the real world have validated the effectiveness of the PhishGuru approach. In a laboratory study we found that embedded training made participants less likely to fall for subsequent phishing attacks. However, the current practice of employers and

service providers sending out security notices did little to protect users from phishing attacks as most users do not read these messages carefully, if at all [6]. In another laboratory study we found that our PhishGuru cartoon was an effective training mechanism when sent as part of an embedded training message, but not when sent directly via email [7]. In a field study conducted with employees of a telecommunications company, we found that PhishGuru can effectively train people in a real-world setting [9]. In another real-world PhishGuru study, we showed (1) users trained with PhishGuru retain knowledge even after 28 days; (2) adding a second training message to reinforce the original training decreases the likelihood of people giving information to phishing websites; and (3) training does not decrease users' willingness to click on links in legitimate messages [5].

Figure 1 presents one of the generic PhishGuru designs that I developed. Studying the landscape of phishing, I developed various instructions and designs to convey the instructions. We maintain a website with the PhishGuru interventions that we develop.<sup>1</sup> I supervised three undergraduate and two graduate (masters) students at Carnegie Mellon University in developing these designs and testing these designs in laboratory and in the real world. PhishGuru is currently being commercialized by Wombat Security Technologies.<sup>2</sup>

### *Anti-Phishing Phil*

In addition to my research on PhishGuru, I am also part of a team developing Anti-Phishing Phil. Phil is an interactive game that teaches users how to identify phishing URLs, where to look for cues in web browsers, and how to use search engines to find legitimate websites [10]. Figure 1 presents a screenshot from the Anti-Phishing Phil game. We maintain a version of the game for public.<sup>3</sup> Around 100,000 people have played this game since October 2007. Novice users who played the game showed the greatest improvement [8]. Anti-Phishing Phil is also currently being commercialized by Wombat Security Technologies.

### *Other research*

In addition to PhishGuru and Phil, I have also studied and developed an online trust model [1]. I populated this model of user behavior with qualitative data from interviews with expert and non-expert computer users. I specifically modeled the way users make decisions in seven different online scenarios, focusing primarily on phishing attacks. Using the model and the interview data, I found similarities and differences in expert and non-expert trust decision-making. Results from this study have helped me tremendously in designing training materials for PhishGuru [2].

I have also researched cultural aspects of privacy. In particular, I studied the perception of privacy in India through surveys and interviews. I compared the privacy perception in the US and in India. We found similar difference in willingness to trust businesses and the government with personal information. Our results suggest that the Indian high tech workforce may not be sufficiently aware of privacy issues, and that the outsourcing industry and international businesses may need to provide privacy training to their workers [4].

---

<sup>1</sup><http://www.phishguru.org/>

<sup>2</sup><http://wombatsecurity.com/>

<sup>3</sup>[http://cups.cs.cmu.edu/antiphishing\\_phil/new/index.html](http://cups.cs.cmu.edu/antiphishing_phil/new/index.html)



**WARNING!**

Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

**How you were tricked**

This email is from my bank and it is asking me to update my information. I better click on the link and update it.

**STOP!**  
Don't fall for this scam email.

**Wombank**  
From: service@Wombank.com  
Dear Jane, Your account will be suspended if you do not update your information. <http://www.Wombank.com/update>

**How to help protect yourself**

- 1 Don't trust links in an email.  
<http://www.amazon.com/update>
- 2 Never give out personal information upon email request.  
Name: Jane Smith  
SSN: 123 456789
- 3 Look carefully at the web address.  
<http://www.amazon.com>
- 4 Type in the real website address into a web browser.  
<http://www.amazon.com>
- 5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.  
Credit Card Statement  
For customer service call 1-800-xxx-xxxx
- 6 Don't open unexpected email attachments or instant message download links.  
My Inbox  
Here is the updated document.  
[attachment](#)

**How phishers trick you**

Here is how con artists try to steal your personal information.

**Wombank**  
From: service@Wombank.com  
Dear Jane, Your account will be suspended if you do not update your information. <http://www.Wombank.com/update>

I forged the address to look genuine.  
I threatened the user with an urgent message.  
I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!

Thanks PhishGuru! Where can I learn more?  
Visit [phishguru.org](http://phishguru.org)

**ROUND 1**      **SCORE: 0**      **LIVES:**      **TIME LEFT: 1 : 22**

**Don't trust URLs with all numbers in the front.**

<http://147.91.75.1/ebay/>

**WITH URL REVEALED:** E EAT LEGITIMATE URLS    R REJECT PHISHING URLS    T ASK YOUR PHISH GURU FOR HELP

Figure 1: Top: One of the latest PhishGuru designs, these have proven to be effective in communicating the instructions to people. Bottom: Screen shot from Anti-Phishing Phil. The screen shows a URL being displayed; the lower right corner features a tip from the PhishGuru fish.

## Current Research

In addition, I am working with two other organizations to implement other forms of phishing education. The first is a collaboration with an ISP to add phishing educational materials to their Webmail system. When their filters detect an email as phishing email and when users click on the link in the suspected phishing email, training materials along with other warning messages are presented to the users. On average, my design is being viewed approximately 70,000 times every-day, starting August 2008. Present data in this implementation shows that this methodology may reduce the number of people who follow the link in the email. The second collaboration is with the Anti-Phishing Working Group (APWG) to create a “landing page” with phishing educational materials.<sup>4</sup> APWG is a global association of industry and law enforcement committed to eliminate Internet scams and frauds. APWG has around 3000 individuals and 1700 companies as their members. When victims click on the link in phishing emails and the linked phishing website has been taken down, ISPs and registrars redirect the users to instructional materials instead of a 404 error (page not found) message. These materials explain that the user has just fallen for a phishing attack and explains ways by which they can avoid being victimized in the future. Our preliminary analysis suggests that approximately 70,000 Internet users have been educated by the landing page so far [3].

## Research Agenda

My previous and current research has helped me develop interesting questions for my future work. In the near future, I hope to extend the PhishGuru methodology to other semantic and security attacks such as spam, and malware. I am also interested in applying the design principles that I have developed into other domains.

In the long term, I plan to better understand the trust behavior of Internet users and develop relevant theory and technologies that will help users make better online trust decisions. I intend to develop technologies and policy recommendations to combat Internet threats and frauds. I also plan to study security and privacy issues related to technologies that improve the quality of life (e.g mobile phones, Radio Frequency Identification (RFID) devices). In addition to these specific interests, I am amenable to work on other research opportunities in broader areas of security, human computer interaction, learning science, and economics of information security.

I will seek active collaboration with other researchers and industry in performing my research. I will also continue to interact with researchers at Carnegie Mellon University, and Anti-Phishing Working Group to further advance the field of information security.

---

<sup>4</sup><http://education.apwg.org/r/en/>

# Bibliography

- [1] KUMARAGURU, P., ACQUISTI, A., AND CRANOR, L. Trust modeling for online transactions: A phishing scenario. In *Privacy Security Trust* (2006).
- [2] KUMARAGURU, P., ACQUISTI, A., AND CRANOR, L. F. Expert and non-expert decision making in online trust scenarios. Working paper. Journal version.
- [3] KUMARAGURU, P., CRANOR, L., AND MATHER, L. Anti-phishing landing page: Turning a 404 into a teachable moment for end users. Under review.
- [4] KUMARAGURU, P., CRANOR, L. F., AND NEWTON, E. Privacy perceptions in india and the united states: An interview study. In *The 33rd Research Conference on Communication, Information and Internet Policy (TPRC)* (September 2005).
- [5] KUMARAGURU, P., CRANSHAW, J., ACQUISTI, A., CRANOR, L., HONG, J., BLAIR, M. A., AND PHAM., T. School of phish: A real-world evaluation of anti-phishing training. *Accepted in Symposium On Usable Privacy and Security* (2009).
- [6] KUMARAGURU, P., RHEE, Y., ACQUISTI, A., CRANOR, L. F., HONG, J., AND NUNGE, E. Protecting people from phishing: the design and evaluation of an embedded training email system. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems* (New York, NY, USA, 2007), ACM Press, pp. 905–914.
- [7] KUMARAGURU, P., RHEE, Y., SHENG, S., HASAN, S., ACQUISTI, A., CRANOR, L. F., AND HONG, J. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *e-Crime Researchers Summit, Anti-Phishing Working Group* (2007).
- [8] KUMARAGURU, P., SHENG, S., ACQUISTI, A., CRANOR, L., AND HONG, J. Teaching johnny not to fall for phish. *Accepted in Association for Computing Machinery's Transactions on Internet Technology (TOIT)* (2009).
- [9] KUMARAGURU, P., SHENG, S., ACQUISTI, A., CRANOR, L. F., AND HONG, J. Lessons from a real world evaluation of anti-phishing training. *e-Crime Researchers Summit, Anti-Phishing Working Group* (October 2008).
- [10] SHENG, S., MAGNIEN, B., KUMARAGURU, P., ACQUISTI, A., CRANOR, L. F., HONG, J., AND NUNGE, E. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security* (New York, NY, USA, March 2007), ACM, pp. 88–99. Symposium On Usable Privacy and Security.