



helping organizations combat phishing

<http://wombatsecurity.com/>

March 2011

A Multi-Pronged Approach to Combat Phishing

About Carnegie Mellon University

- Global, private research university with main campus in Pittsburgh and more than a dozen degree-granting locations around the world
- 11,000 students; 84,000 alumni; 4,000 faculty and staff
- School of Computer Science is ranked first in the nation by U.S. News & World Report magazine's "America's Best Graduate Schools"
- Operates CyLab, one of the largest university-based cyber security research and education centers in the U.S.

Carnegie Mellon University (CMU) is one of the world's premier institutions for computer science research and education. It is therefore no surprise that the organization is leading the way in combating phishing attacks with an evidence-based, multi-layered approach.

As part of this approach, CMU has licensed Wombat Security Technologies' complete suite of anti-phishing products. They include a combination of highly effective training tools—PhishGuru, Anti-Phishing Phil and Anti-Phishing Phyllis—and a unique anti-phishing email filter, PhishPatrol, that complements traditional anti-spam and anti-virus filtering solutions. These products, which today are licensed by Wombat for use by millions of users around the world, have been deployed by customer organizations in finance, government, telecom, health care, retail, education, transportation, energy, IT and the service industry.

“The most important thing is to give people the skill set to practice the right behavior. Just making them aware of phishing emails is not sufficient. They need to be able to effectively differentiate between legitimate and fraudulent emails.”

*Mary Ann Blair,
Director of
Information Security,
Carnegie Mellon
University*

Carnegie Mellon is part of a growing number of organizations that are taking a multi-pronged approach to combating phishing.

“Like many organizations, we face continuing threats of credential loss via phishing attacks,” says Mary Ann Blair, CMU's Director of Information Security. In this role, she is responsible for real-time protection of the campus computing and network infrastructure and institutional information—which includes training and awareness.

“We are concerned about all of our constituents—not just staff and faculty but also our students,” says Mary Ann. “These attacks leave individuals personally vulnerable to identity theft. Educating the entire community is part of CMU being a good citizen.”

Colleges and universities are at high risk for two reasons. Higher education is an increasingly popular target for spear phishing, the practice of sending fraudulent e-mails to employees or members within a specific organization. “They are getting very clever about the lure, the phishing email, and the site you land on when you click through,” Mary Ann says.

Further, younger adults are particularly vulnerable. Research conducted at CMU revealed that 18-to-25 year-olds were particularly likely to fall for phishing attacks. “It's important therefore that we raise awareness among our entire user community,” says Mary Ann. “They are our last line of defense.”

PHISHGURU: PRACTICAL TRAINING THROUGH SIMULATED ATTACKS

Raising awareness is an important, but only partial, step in the training process. For users to learn the skills they need to better protect themselves, the training must be provided at the right time, in the right way. That premise is at the core of the success of Wombat's PhishGuru product, which incorporates principles of learning science to teach skills in real time and in context.

A software-as-a-service product, PhishGuru enables IT administrators to train users by sending them simulated phishing emails. When users fall for one of the simulated emails, the system doesn't just record their error—it also pops up real-time training that teaches users how to avoid falling for similar attacks in the future.

“The traditional way to train users about phishing is to scare them—but that does not give them the skill set to act correctly,” says Mary Ann. For one thing, scientific studies show that employees are not motivated to pay attention to static cyber security training emails. When users are trained with this method, or via classroom lectures, they not only continue to fall for phishing emails, they also grow afraid of emails that are legitimate.

Instead of using scare tactics, PhishGuru provides the training via a fun, informative and effective cartoon. In addition, the software includes reporting functionality to help organizations track their users' progress across multiple training campaigns.

Results show it works. In an early PhishGuru campaign run at CMU with 500 participants, those who fell for the simulated attack spent an average of just two minutes reading the training cartoon. Yet that single round of training reduced the number of those participants falling for subsequent phishing emails by 50%. Users read the cartoon, and they remembered it. In a follow-up campaign run 28 days later to test the long-term effect of PhishGuru training, Mary Ann found that her users had retained the knowledge they had learned, with the chance of participants falling for the follow-up simulated attack remaining 50% lower.

What about acceptance? Do users report feeling tricked or hold another negative reaction to this method? The answer is no.

“We were concerned that they would be resistant,” says Mary Ann, “but the vast majority of participants responding to our post-study survey indicated that they wanted CMU to continue using it. So we purchased a license for the PhishGuru tool.”

Multiple rounds of PhishGuru training are even more effective so, during recent months, the university launched two customized campaigns targeting the student population. “With cyber criminals continuing to develop increasingly customized phishing emails, it is critical that we continue training our user population with regular campaigns,” adds Mary Ann.

ANTI-PHISHING PHIL AND ANTI-PHISHING PHYLLIS: 10-MINUTE GAMES THAT OUTPERFORM HOUR-LONG LECTURES

Because simulated phishing attacks cannot be launched by the university every week, Mary Ann supplements her PhishGuru campaigns with two unique training games also developed by Wombat: Anti-Phishing Phil and Anti-Phishing Phyllis. These tools represent CMU's second layer of training against phishing attacks.

In contrast to PhishGuru, which presents users with a single training example at a time, these games enable members of the campus community to cover a larger number of examples in a matter of just a few minutes.

Anti-Phishing Phil 2.0 is a SCORM-compliant game that teaches users to recognize fraudulent URLs. During about 10 minutes of play, the user is asked to judge 32 different URLs from a large selection within the game's database. The newest release of the game reflects trends such as the significant increase of phishing attacks taking place through social networks.

Like PhishGuru, the games come with extensive reporting functionality that enables security professionals to track the performance of their users. The 508-compliant versions are designed for users with disabilities. Like all Wombat training solutions, Anti-Phishing Phil is customizable—and has been shown to significantly reduce the likelihood of users falling for future phishing attacks.

According to the Scientific American article “How to Foil ‘Phishing’ Scams,” which featured Anti-Phishing Phil, “the ability of subjects who had played the game to distinguish legitimate URLs from fraudulent ones improved nearly twice as much as that of those trained with standard materials.”

CMU launched the game almost a year ago. “We have it implemented in a way so that anyone in the CMU community may access it,” says Mary Ann. To further reinforce the concepts, Anti-Phishing Phil has been incorporated into the core curriculum of the university. All freshmen are required to complete a course called “Computing at Carnegie Mellon.” As part of that online learning environment, freshmen will play the game and be tested on their mastery of the material.

“Our most vulnerable population is our freshmen,” says Mary Ann. “Over time, as all freshmen go through this process, all students will be trained in these skills.”

Complementing Anti-Phishing Phil is Anti-Phishing Phyllis, a training solution that CMU will deploy later this year. This 10-minute game teaches users to spot phishing traps in fraudulent emails. Traps include fake links, malicious attachments, cash prizes, “respond-to” emails asking for sensitive information and others. As in Anti-Phishing Phil, this game provides immediate feedback to players about the traps they miss so they learn to better protect themselves.

PHISHPATROL: CATCHING WHAT SPAM AND VIRUS FILTERS MISS

CMU's Electrical and Computer Engineering Department was first to deploy PhishPatrol at the university. The department's email filtering solution is state-of-the-art and combines grey listing with some of the best anti-spam and anti-virus filters available today. Yet, many phishing emails would continue to get through.

Most email filters rely heavily on blacklists to catch phishing emails. These lists are systematically several hours behind—sometimes more. Because most users read their email within a few hours of its arrival, standard filters

“PhishPatrol was able to improve our filtering of phishing emails with zero false positives, minimal configuration and no noticeable load increase.”

*Lou Anschuetz,
Network Manager,
Carnegie Mellon
University*

cannot keep pace. In contrast, Wombat's PhishPatrol uses advanced machine learning techniques and a unique combination of email features to detect phishing. This enables the filter to catch many phishing emails that go undetected by other filters, including many zero-hour attacks.

PhishPatrol is intended to supplement an organization's existing email filters rather than replace them. As such, it is designed to be easy to deploy alongside anti-spam and anti-virus filters.

"PhishPatrol was able to improve our filtering of phishing emails with zero false positives, minimal configuration and no noticeable load increase," says Lou Anschuetz, CMU's Electrical and Computer Engineering network manager.

A SUITE OF TOOLS TO EMPOWER USERS, PROTECT THE ENTERPRISE

Mary Ann Blair believes this multi-layered "counter attack" makes the most sense for the enterprise—and the people—she protects.

"Wombat is very close to home, so of course my opinion is a bit biased," she says. "However, given the background of the company, separate and apart from CMU, theirs is very much a data-driven approach. The products really are about addressing the concerns people are finding in internet security.

"Also, their products are the result of research that has gone through the scientific peer review process, and the results of their studies have been presented at peer-reviewed conferences. That is pretty unique and says a lot about the effectiveness of their solutions"

In fact Mary Ann has been so impressed with Wombat's tools that she decided to share her experience with her peers at the EDUCAUSE 2010 annual conference, where she explained CMU's success using Wombat products, especially PhishGuru.

"At the conclusion of the talk, I had a line out the door of folks who wanted to know how we did what we did," she says.

In essence, Wombat did what the most clever phishers do: Pay close attention to user behavior and capitalize on those observations to influence desired behaviors.

"The most important thing is to give people the skill set to practice the right behavior," says Mary Ann. "Just making them aware of phishing emails is not sufficient. They need to be able to effectively differentiate between legitimate and fraudulent emails."

"That is our goal, to give them the skills to take the right action. And our results show that it works."