Study suggests users pay more attention to Internet safety than previously assumed

February 28 2014, by Katherine Shonesy

Internet users face a barrage of information with each click, some of it designed to compromise security and privacy. Spammers hope, and security researchers have warned, that users cannot distinguish legitimate websites from dangerous ones and do not heed browser safety warnings.

However, new research from University of Alabama at Birmingham suggests that users pay more attention to Internet safety than previously assumed. In a paper that won the "Distinguished Paper Award" at the 2014 Network and Distributed Systems Security Symposium, researchers used a novel methodology to gain new neurological insights into how users face security questions and how their personalities might affect their performance.

Nitesh Saxena, Ph.D., associate professor in the Department of Computer and Information Sciences and a core member of the Center for Information Assurance and Joint Forensics Research, wondered what was happening in Internet users' brains when they encountered malware warnings or malicious websites.

"Many computer-based lab studies on user-centered security have concluded that users do not pay attention to these tasks and are ill-equipped to pay attention to security warnings," Saxena said. "I had been taught for years that users are careless when it comes to security endeavors."

However, security studies in lab settings show different results than a

recent study based on real-world user data, he says.

He teamed up with Rajesh Kana, Ph.D., associate professor of psychology, and UAB graduate research assistants Ajaya Neupane (lead student author) and Michael Georgescu, as well as Keya Kuruvilla, a Department of Psychology student, to use brain imaging to discover what is really happening in users' brains as they encounter security questions.

Users were given two tasks. First, they were shown intermingled examples of popular websites' real login pages and fraudulent replications of those pages and were asked to determine which were real and which were fake - phishing - sites. Users were then asked to read several sample news articles and were interrupted by pop-ups that contained either benign information or warnings about malware, software created to obtain unauthorized access to a computer's resources and collect information.

Using a functional magnetic resonance imaging, or fMRI, machine, researchers measured users' accuracy while tracking their brain activity. Results showed activation in areas of the brain associated with attention, decision-making and problem-solving. Activity in the brain's decision-making regions carried across both tasks, suggesting that accuracy at one task could predict accuracy at the other.

"For both tasks we found brain activity, so people are not careless," Saxena said. "But whether or not their decisions are valid is a different situation."

Accuracy in the malware warning task was about 89 percent, and the fMRI scans showed high brain activity in regions associated with problem-solving and decision-making.

"In the warning task, people seem to make extra effort to make decisions," Saxena said. "When they were subject to warnings, there was also activity in language comprehension areas. Warnings trigger some sort of thought process in people's brains that there is something unusual going on."

Accuracy in identifying real versus fake websites was low at only about 60 percent - only 10 percent better than a random guess, though participants showed activation in brain regions associated with decision-making.

"In the phishing task, users didn't do very well," Saxena said. "That may be because they don't know what to look for. When they look at a website, they might be paying attention only to the look and feel of the website instead of the URL, which is often a real indicator."

Researchers also had users complete a personality assessment to measure their impulsiveness, and the fMRI results showed differences in how highly impulsive users behaved.

"Not all individuals are alike," Saxena said. "We found a negative correlation of impulsivity and brain activity. Highly impulsive people probably just hit 'yes' when they are stopped by a malware warning asking if they want to proceed. This is interesting because it offers a way to predict how people may perform in security tasks based on impulsivity scores."

The relationship between personality traits like impulsivity and brain responses was especially interesting, Kana says.

"Participants with greater impulsive traits showed less brain activity in key decision-making areas of the brain during security decisions," Kana said.

The study could help security programmers focus their attention on designing better warning systems, and network managers target their security training at users who tend to be impulsive, Neupane says.

Provided by University of Alabama at Birmingham