Home-computer users at risk due to use of 'folk model' security

May 24 2011

(PhysOrg.com) -- Most home computers are vulnerable to hacker attacks because the users either mistakenly think they have enough security in place or they don't believe they have enough valuable information that would be of interest to a hacker.

That's the point of a paper published this month by Michigan State University's Rick Wash, who says that most home-computer users rely on what are known as "folk models." Those are beliefs about what hackers or viruses are that people use to make decisions about security – to keep their information safe.

Unfortunately, they don't often work the way they should.

"Home security is hard because people are untrained in security," said Wash, an assistant professor in the Department of Telecommunication, Information Studies and Media. "But it isn't because people are idiots. Rather they try their best to make sense of what's going on and frequently make choices that leave them vulnerable."

In his paper, published in the proceedings of the *Symposium on Usable Privacy and Security*, Wash identified eight folk models of security threats that are used by home computer users to decide what security software to use and which advice to follow.

These models range from the vague and generic – "viruses are bad" – to the more specific – "hackers are burglars who break into computers for

criminal purposes."

Adding to the problem, Wash said, is that people who rely on folk models for computer security don't necessarily follow security advice from credible experts. This is because they either don't understand the advice or because they believe the security advice isn't relevant to them.

Knowing what people believe or discount can help the experts help the users.

"The folk models we describe begin to provide an explanation of which expert advice home computer users choose to follow and which advice to ignore," Wash said. "By better understanding why people choose to ignore certain pieces of advice, we can better craft that advice and technologies to have a greater effect."

It's also important, he said, that security experts do a better job of explaining the threats that home computer users face.

"Without an understanding of threats, home-computer users intentionally choose to ignore advice that they don't believe will help them," Wash said. "Security education efforts should focus not only on recommending what actions to take, but also emphasize why those actions are necessary."

Provided by Michigan State University