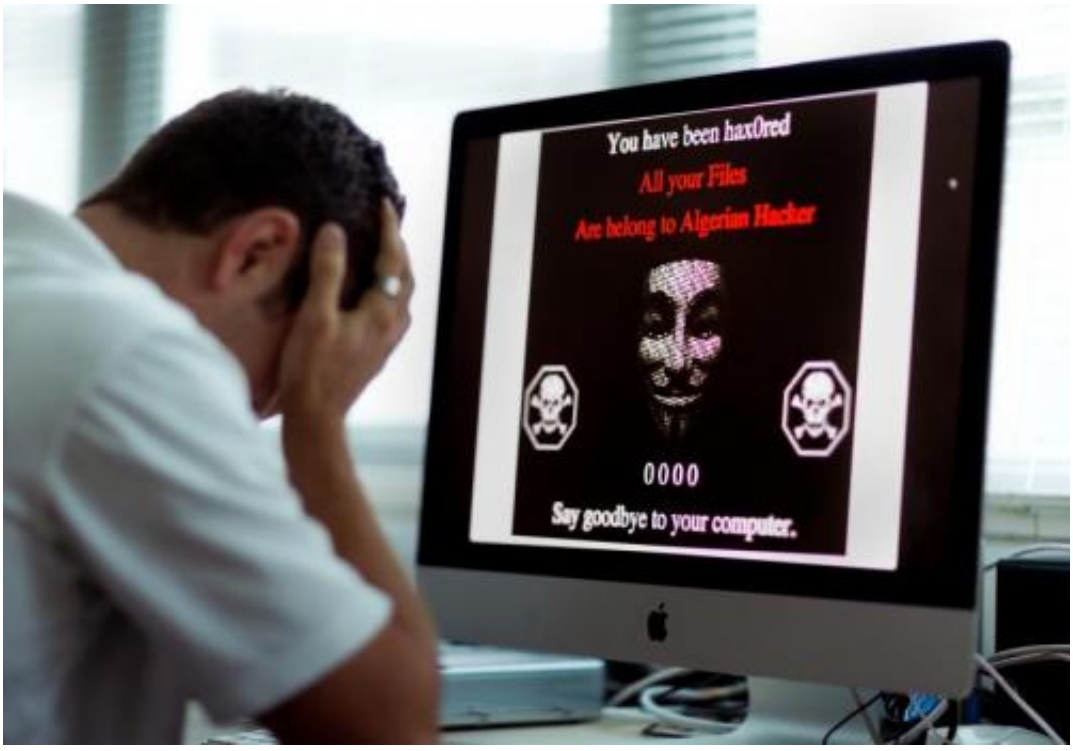
Don't get hacked! Research shows how much we ignore online warnings

November 20 2014



Student sees the hacking screen that researchers used to study online security warnings. Credit: Jaren Wilkey/BYU Photo

Say you ignored one of those "this website is not trusted" warnings and it led to your computer being hacked. How would you react? Would you:

A. Quickly shut down your computer?

B. Yank out the cables?

C. Scream in cyber terror?

For a group of college students participating in a research experiment, all of the above were true. These gut reactions (and more) happened when a trio of Brigham Young University researchers simulated hacking into study participants' personal laptops.

"A lot of them freaked out—you could hear them audibly make noises from our observation rooms," said Anthony Vance, assistant professor of Information Systems. "Several rushed in to say something bad had happened."

Fortunately for the students, what they saw—a message from an "Algerian hacker" with a laughing skull and crossbones, a 10-second countdown timer and the words "Say goodbye to your computer"—wasn't real. What was real was that all of the participants got the message by ignoring web security warnings.

Vance and BYU colleagues Bonnie Anderson and Brock Kirwan carried out the experiment to better understand how people deal with online security risks, such as malware. They found that people say they care about keeping their computers secure, but behave otherwise—in this case, they plowed through malware warnings.

"We see these messages so much that we stop thinking about them," Vance said. "In a sense, we don't even see them anymore, and so we often ignore them and proceed anyway."

For the study, researchers first asked participants how they felt about online security. Then, in a seemingly unrelated task, participants were told to use their own laptops to log on to a website to categorize pictures

of Batman as animated or photographed. (Students were told their image classification project was being used to check the accuracy of a computer algorithm to do the same task.)

As participants clicked through the image pages, warning signs would randomly pop up indicating malware issues with the site they were accessing. If they ignored the message enough times, they were "hacked."

"A lot of people don't realize that they are the weakest link in their computer security," said Kirwan, assistant professor of Psychology and Neuroscience at BYU. "The operating systems we use have a lot of built-in security and the way for a hacker to get control of your computer is to get you to do something."

Kirwan's role in the research added another fascinating layer: Using his expertise in neuroscience, Kirwan carried out an additional experiment on subjects using EEG machines to measure brain responses to risk.

While results showed that people say they care about web security but behave like they don't; they do behave in-line with what their brains say. In other words, people's brainwaves better predict how risky they are with online security.

"We learned that brain data is a better predictor of security behavior than a person's own response," Vance said. "With neuroscience, we're trying to understand this weakest link and understand how we can fortify it."

Anderson, an associate professor of Information Systems, echoed the need to do so, quoting security expert Bruce Schneier: "Only amateurs attack machines; professionals target people."

The current study was published recently in the *Journal of the Association for Information Systems*.

Provided by Brigham Young University