PHYS.ORG

New technology won't prevent information security breaches, say ISU experts

February 11 2010

(PhysOrg.com) -- The story's become all too familiar in today's digital world. A security breach provides a hacker access to a computer system containing the personal information of 80,000 people.

This time, the hacker gained entry to personal information through the licensing database of the Iowa Racing and Gaming Commission. But it could have been another state's computer system, or a finance company's system, or your home computer.

Would new technological advancements -- such as retina, iris, or fingerprint scans, like those popularized in the 2002 film "Minority Report" -- prevent the security breach? Three Iowa State University information security experts agree that the answer is "no."

New technology's impact on identity theft

Qing Hu, a professor and chair of logistics, operations and management information systems at Iowa State, says those new technologies won't even make a dent on the identity theft problem.

"Identities are sold around the world quickly after they are stolen through online auction sites operated by organized crime or hackers, and they are used for a number of purposes -- most of which do not need a personal presence where a retina scan might be used," said Hu, who has been conducting research on corporate information security management and user behavior toward information security technologies since 2005.

"They [stolen identities] can be used to apply for new credit cards, making duplicate cards for online purchases of digital services and products where physical delivery is not needed -- online games, pornographic material, music download, fake account for money laundering, etc.," he said. "It is rare that a criminal would take a fake ATM card to go to a physical machine to take cash out, knowing that almost all ATMs today have cameras to record every transaction."

Steffen Schmidt, a University Professor of political science who is also a researcher in ISU's Center for Information Protection, shares Hu's information security outlook amid new technology. The co-author of two books on preventing identity theft -- "Who Is You: The Coming Epidemic of Identity Theft" (The Consortium, 2005) and "The Silent Crime: What You Need to Know About Identity Theft" (Twin Lakes Press, 2008) -- Schmidt predicts identity theft will only escalate with technological advancements.

"Vulnerability of electronic devices to hacking, malware, and 'zombiefication' will explode into a virtually uncontainable crisis for all digital, networked device manufacturers as soon as a truly major incursion takes place -- for example, into an entire smart phone system," he said. "When that happens, device manufacturers and their software partners will finally be forced to step up to the plate and initiate more secure Internet access than the hopelessly weak 'secret' passwords."

Schmidt predicts that biometrics will quickly "up armor" and eventually replace passwords for most transactions and for computer access. "If you can stick a credit card in a slot and start pumping gas in less than 10 seconds, you can scan an eye or a fingerprint in the same time in the future," he said.

The problem with biometrics

But that's not necessarily a good thing, according to Doug Jacobson, director of the ISU Information Assurance Center and a University Professor of electrical and computer engineering.

"Technologies like fast retina scanners are designed to tie a person to a digital identity," Jacobson said. "That is one of the weaknesses in the digital ID system which is called authentication -- connecting a person with a digital ID. Another weakness is how the digital ID is protected and misused. If you re-authenticate your ID every time you use it, then it is safer, but it is not as user-friendly."

Hu also sees both the retina scanner and fingerprint devices being intrusive to individual privacy, and therefore likely to be rejected by the population at large. And he also doesn't have great confidence that they'll be more effective against information security breaches.

"Given the current global network and connectivity and the degree of e-commerce activities, it is almost impossible to identify one or two technologies that can make a significant dent in the identity theft problem," Hu said.

"On the other hand, the global connectivity may also offer the best opportunity to combat identity theft," he continued. "For instance, a global data exchange of some sort can quickly identify that the online transactions requested in one country actually use an identity of a resident in another country who has just used his or her card in a local store."

At this point, Hu reports that banks and credit card issuers are not sharing such information, creating opportunities for thieves and criminals around the world.

Provided by Iowa State University

Citation: New technology won't prevent information security breaches, say ISU experts (2010, February 11) retrieved 24 April 2024 from https://phys.org/news/2010-02-technology-wont-breaches-isu-experts.html