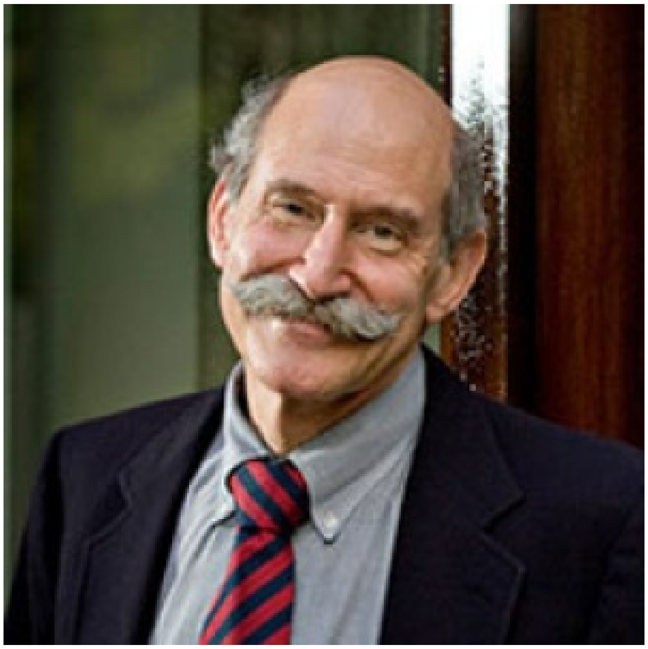
PHYS.ORG

Computer users circumvent password security with workarounds, according to study

April 18 2014, by Jacquie Posey



Ross Koppel

(Phys.org) —When workers and organizations circumvent computer passwords and security rules, they unwittingly open the door to hackers, according to a study co-authored by Ross Koppel, an adjunct professor of sociology at the University of Pennsylvania.

Koppel is also an affiliate professor at Penn's Perlman School of

Medicine, a senior fellow at the Leonard Davis Institute of Penn's Wharton School and a senior investigator at the Department of Computer and Information Science in Penn's School of Engineering and Applied Science.

The study, "Circumvention of Security: Good Users Do Bad Things," is published in the *Institute of Electrical and Electronic Engineers Security & Privacy*.

With co-authors Jim Blythe of the University of Southern California and Sean W. Smith of Dartmouth College, Koppel studies what people actually do when working online without following computer security experts' rules. The researchers found that "circumvention of the rules is the norm."

Koppel's research generally focuses on health-care IT workarounds that doctors and nurses are required to perform when computer system rules are clunky or non-responsive to work flow. This research on cyber security is an outgrowth of that work. The researchers found that often the rules on passwords are so "onerous" or "cumbersome" that workers must find ways to circumvent them to perform their duties.

The research team conducted a series of in-depth interviews with cyber-security experts, chief information and chief medical information officers, IT workers, computer users and managers. They asked questions about perceptions of computer security rules, logic, protocols, norms and actual practice.

"These interviews expose the often irrational security controls and subsequent workarounds, such as password sharing, made-up data to allow access to restricted parts of systems and ignoring warnings about invalid or obsolete programming," Koppel said.

They discovered "innumerable" vulnerabilities that are generated not by hackers, but by inflexible or illogical requirements of cyber security regulations.

Examples included:

- Having to change passwords every 90 days, and requiring a new password. They found that workers in the defense industry would call their help desk, saying they forgot their passwords. The act of resetting the passwords negated the history, thus enabling them to reuse their old password forever.
- Users would circumvent timeouts on their systems by putting Styrofoam cups over proximity detectors to trick the system into believing they had never left.
- To circumvent a hospital's rules on exfiltration of medical images, a doctor would take a screenshot and drop the image into conventional and unprotected email.
- A superior insisted on not using a standard trust root for the enterprise's SSL servers, and users were trained to ignore warnings about invalid SSL certificates, the software at issue with the Heartbleed bug.

The study was conducted for the Army Research Office.

More information: Blythe, J.; Koppel, R.; Smith, S.W., "Circumvention of Security: Good Users Do Bad Things," *Security & Privacy, IEEE* , vol.11, no.5, pp.80,83, Sept.-Oct. 2013. DOI: 10.1109/MSP.2013.110

Provided by University of Pennsylvania

Citation: Computer users circumvent password security with workarounds, according to study (2014, April 18) retrieved 2 May 2024 from https://phys.org/news/2014-04-users-circumvent-password-workarounds.html