Security Snippets — May 2014

A monthly compendium of info security news

Hot Attacks	Ransomware is continuing to infect PCs and is now starting to infect Android devices. Ransomware is a type of malicious software that "locks up" your computer and encrypts all your files until you pay a fee (usually around $300). On a PC, you can get infected when you open a malicious email attachment, visit a compromised website, or click on a malicious ad. On an Android device, when you visit a compromised website, the site redirects you to a porn site that "entices" you to download the malicious software. To protect your devices, follow the usual security best practices (these are generally easier to do on a PC than a smartphone). Keep the device patched, run antivirus, and backup your data. You may need to restore your system if you get infected. True story: The PC of the grandmother of one of my fellow security professionals got infected with ransomware. Grandma refused to pay the ransom and bought herself a new PC.
Cybercrime / Hacking	From cyber-jacking and car-sploiting to human malware, here's an interesting article about eight future cyber crimes. Don't panic, and do insist manufacturers build security and privacy into their products. For more info, see Hackers and Headlines, starting on slide 35.
Home / Personal Issues	According to a recent survey, four in 10 children fear they are addicted to the Internet. Two thirds of 11 to 17-year-olds take their tablet, smartphone or laptop to bed with themselves to talk to friends online, play games, and watch films. Learn about cyber bullying and internet safety. One dad wrote a letter to his daughter about internet privacy and security. It's very well written. You might send a copy of this to your child (or to your parents!).
Politics / Legislation	On April 29, the Supreme Court heard arguments about whether police can search an arrested criminal suspect's cell phone without a warrant. The issue is whether the search violates the Fourth Amendment ban on unreasonable searches, since cell phones contain so much personal information. Under court precedent, police are permitted to search a defendant at the time of an arrest without a warrant, primarily to ensure the defendant is not armed and to secure evidence that could otherwise be destroyed. Their ruling is expected by the end of June.
Privacy / ID Theft	A Princeton sociology professor actively tried to keep her internet browser from figuring out she was pregnant. She called friends and family to announce the pregnancy rather than write anything on Facebook or social media. She asked them to do the same, but had to un-friend an uncle who broke the rule. (Facebook is one of the most-closely "mined" areas for personal information.) She paid for everything with cash and used a new email address and Amazon coupons (bought with cash) when she had to buy online. She even rented out a shipping locker so her online purchases weren't shipped to her home address. She did all this both as an experiment and to avoid the invasive marketing tactics used by firms who use internet data collection as a way to predict spending patterns. Information about normal people sells for 10 cents per individual, but marketing companies can charge up to $1.50 per pregnant woman.
Best Practices / Risk Mgmt	Burglars targeted a draft board office in Delaware to steal Selective Service records. During their casing, they noticed that the interior door that opened to the draft board office was always locked, and they couldn't pick the lock. So several hours before the burglary was to take place, one of them wrote a note and tacked it to the door they wanted to enter: "Please don't lock this door tonight." When the burglars arrived, the door was obediently left unlocked. By the way, this great example of social engineering happened in 1971.

Quote of the Month	A computer once beat me at chess, but it was no match for me at kick boxing. — Emo Philips
Bonus!	It's generally not considered a good idea to poke at hackers, but it's funny to watch. Security bigwig, Ira Winkler spoke at the recent RSA security conference. He describe the methods used by the Syrian Electronic Army, identified some of its members, and called the SEA "cockroaches of the Internet." So they retaliated by hijacking some of the Wall Street Journal's twitter accounts, posted a picture of a cockroach with Ira's head and called him a cockroach. Ira responded with a blog post describing how the "simple and basic" attack was carried out (insulting the SEA's hacking skills). Ira told CNN that the Syrian hacktivists are "imbeciles" and "more ants than cockroaches." So get some popcorn. I expect this feud to get even more entertaining.
Questions & Feedback	Security Snippets is brought to you by Information Technology Services' Information Security & Privacy office and your department. Its purpose is to help you learn more about information security and privacy so you can better protect yourself and your family, as well as the City of Phoenix and our citizens. Contact us at ispo@phoenix.gov with any questions and to provide feedback. Learn more at phoenix.gov/infosec. Want more security-related info? ISPO distributes a report every weekday of current news collected by Department of Homeland Security (and ISPO adds the occasional snarky comment). Just send an email to ispo@phoenix.gov and ask to be added to the DHS report distribution list.