Security vs. Privacy:
When it comes to cyber security trust no one

By Robert Rivard
Editor in Chief, San Antonio Express-News

Effective immediately, I've got cyber security religion. It's scary out there, and I'm going on the defensive. You should, too.

Everybody else is kicking back on a Friday night, sipping a margarita, hanging with friends, planning Super Bowl Sunday. Me? I'm changing passwords, downloading patches for outdated programs, running redundant anti-virus programs, sniffing for malware.

All week I've been enjoying my new MacBook Pro, but after today, the party's over. I trust no one. For starters, I've gone into my Word program and changed the name of one of my cleverly named documents, "mypasswords.doc." Guess what I kept in there?

Hackers around the world apparently are laughing at me, my identity theft just a few keystrokes away for some shadowy mafia figure in Romania, or maybe he's not an Eastern European gangster, but just a mischievous IT nerd in one of the local high school computer labs.

Apparently there is no way of telling.

In fact, today's cyber adversary could be tomorrow's protector: pimpled troublemaker today, entrepreneur millionaire before he's 30 years old, with his own company that helps defend clueless companies run by people like you and me against hackers.

I thought my 500 closest friends on Facebook could be trusted with my periodic updates and photos. How naïve. My friends happen to be cool. But I never stopped to consider the sheer malice of the friends of friends of my friends, whoever they are.

Parents, it's no longer a matter of taking precautions to make sure your children are not exposed to the wrong influences on the Web — like porn sites, for example. Go ask the cyber-savvy kids to help you tighten your own shoddy security. If you're lucky, they'll help before your tax returns spill onto the Internet.

We are such easy prey.

That's what I learned Friday evening at the Charline McCombs Empire Theater, where I moderated a panel of cyber security experts for a full house of visiting members of the Texas Lyceum, which is holding its statewide meeting in San Antonio this weekend. **The hour-long discussion was aired on public television stations around the state. Cyber security - the next big thing - is becoming front and center for the American public.**

 It's an issue that looms as large for the U.S. government, military and law enforcement community as the average Joe who is worried about someone hacking into his American Express account. The Chinese government just hacked into Google in pursuit of dissidents (whoops, did I forget to write "allegedly"?), and company officials are turning to the National Security Agency for help in tracing the attack and preventing future cyber assaults.

Truth is, it takes a sense of humor to take in stride the terrible risks that confront us as we enter an era of total digital dependence. The average individual simply cannot calculate the risk or respond to threats that are so invisible I wasn't sure I trusted the panelists I was interviewing.

They convinced me they were right. I'm cleaning house. I'm not saying you are part of the problem, but if I "unfriend" you on Facebook or "unfollow" you on Twitter, you'll understand. It's nothing personal.

ABOUT THE AUTHOR:

Robert Rivard is the editor of the Express-News. Rivard has worked for five different Texas newspapers over his 27-year career, and also served as a foreign correspondent in Central America and as a senior editor at *Newsweek* magazine in New York. In April 2000, he was chosen by *Editor & Publisher* magazine as its first annual Editor of the Year.
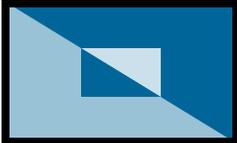
Security vs. Privacy:
Texas Center tries to mitigate risk with real lessons

By Rebekah Sills Lamm
Texas State University School Safety Specialist

The Texas School Safety Center was created in 1999, partly in response to the Columbine school shooting, as a centralized location for technical assistance and training for Texas school districts concerning topics related to school safety. In addition to school safety, the Texas School Safety Center also focuses on tobacco prevention and youth leadership. Our services are free to schools, as we are funded by the legislature through Texas State University – San Marcos.

The funding for my position came in 2007 from Senate Bill 136, which required the Texas School Safety Center (TxSSC) to create a program providing instruction about Internet safety, including cyber bullying, in collaboration with the Office of the Attorney General.

Upon joining TxSSC in April 2008, I developed an awareness training for youth and adults about internet safety and began delivering it around the state. In 2009, I spoke to more than 2,000 youth and about 1,300 adults, spanning rural and urban areas, low and high socioeconomic status, and every Texas demographic. I'd like to share with you a few observations I've made as I traveled around the state.

Students, for the most part, do not understand the terms adults give these topic, such as cyberbullying or online solicitation. This is a major cause of the knowledge gap between adults and youth. More importantly, students do not separate and categorize their problems the way adults do for them. They do not keep a drug file and a bullying file; it's the life they live and everything is connected to their relationships.

Another area of concern that widens the gap is privacy. The definition of privacy has certainly changed for our young people creating a space for adults and youth to clash. However, it's important to note that youth treasure their privacy and will fight for it, even if it looks different to them than to adults.

Perhaps not the most serious, but one of the biggest risks young people face online is posting pictures and content in a way that can negatively impact their futures. We've heard countless stories of youth who've lost scholarships, jobs, and opportunities to better their lives because of what they have posted online.

Along the same lines, youth do not recognize online risks the same way adults do, which hurts the effectiveness of our messages.   One major goal at TxSSC is to incorporate youth input so that we reach their peers more effectively. In my experience they want real life stories and examples of real life consequences. They also need tangible steps they can take to contribute to their own safety, questions they can ask themselves, and strategies to make good decisions about what they post online.

Here's a good start, courtesy of Nancy Willard at The Center for Safe and Responsible Internet Use:
What's the situation? Who's involved? How would I feel if my actions were reported in a newspaper?
Would it be okay if I did this in Real Life? How would this reflect on me? For more information about TxSSC or youth risk online, please contact me at rs53@txstate.edu or 512-245-8082.

ABOUT THE AUTHOR:

Rebekah Sills Lamm is a School Safety Specialist at the Texas School Safety Center at Texas State University - San Marcos. www.txssc.txstate.edu.
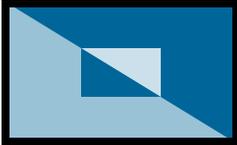
Security vs. Privacy:
Is There a Trade-Off and Can the Trade-Off be Avoided?

By Nicole Beebe, Ph.D.
Assistant Professor at the University of Texas at San Antonio

In the months, perhaps even the first couple of years following 9/11, Americans seemed willing to prioritize security over privacy—even willing to achieve security *at the expense of* privacy. Prevailing opinion was that a trade-off exists between privacy and security, as evidenced by a significant drop in privacy expectations in America (Taylor, 2003).

Shortly after the attacks, Bruce Schneier, a leader in the information security field, concluded that people seemed to view the trade-off as a *fait accompli* – a fact, or condition that cannot be undone (Schneier 2001). What caused this shift in privacy expectation? Is it truly that Americans believe concerns for personal security and safety trump privacy, as the above discussion suggests? Is it that less privacy is simply an irreversible by-product of life in the twenty-first century?

In a contrasting view, a 2007 poll suggests the drop in privacy expectation is due to technological advancement and generational effects (Government Technology, 2007). Ninety-one percent (91%) of respondents agreed privacy expectations have declined with increased technological advancements. The survey also showed age is highly and inversely correlated with the perception of what constitutes a privacy invasion.

Another view suggests that the nature of this change is economic. A 2008 Consumer Reports Poll (Kelsey and McCauley, 2008) indicates consumers' privacy expectation on-line is *increasing*. According to the poll, "82 percent of consumers are concerned about their credit card numbers being stolen online, while 72 percent are concerned that their online behaviors were being tracked and profiled by companies."

Based on this evidence, it seems that expectations of privacy are highly dependent upon contextual factors – personal security, technological convenience, social vs. professional vs. commerce environments, etc. So, just what is important to people when it comes to 'privacy?' Further, why do we want to keep our info private? "Information forms the intellectual capital from which human beings craft their lives and secure dignity... [That] capital is impaired whenever [people] lose their personal information without being compensated for it, when they are precluded access to information which is of value to them, when they have revealed information they hold intimate, or when they find out that the information upon which their living depends on is in error" (Mason, 1986).

Based on this, we identify five issues central to privacy concerns in the information age. The issues include: (1) extensive collection of personally identifiable information, (2) internal, unauthorized secondary use of personal information, (3) external, unauthorized secondary use of personal information, (4) errors in personal information stored, and (5) improper access to personal information stored (Smith et al., 1996).

Last, we should ask, is a trade-off even necessary? In the same talk where Schneier said people viewed the trade-off as a *fait accompli*, he was quick to caution Americans against accepting this trade-off too eagerly, suggesting there are ways to achieve privacy and security simultaneously. He argues these concepts are not mutually exclusive and both can be achieved if considered early on and designed into the system from the beginning.
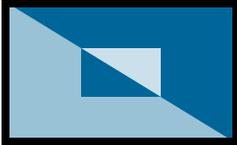
Security vs. Privacy:
Is There a Trade-Off and Can the Trade-Off be Avoided?

When security is 'tacked-on' to an already fully designed and operational system, the method for achieving it is often more invasive from a privacy perspective. Designing both security and privacy in from the beginning can lead to a more mutually reinforcing system from the perspective of operations, security, and privacy (Clark et al.).

REFERENCES:

Clark, Jan Guynes, Nicole Lang Beebe, Karen Williams, and Linda Shepherd, "Security and Privacy Governance: Criteria for Systems Design," *Journal of Information Privacy and Security* (forthcoming).

Government Technology (2007) http://www.govtech.com/gt/articles/103678

Kelsey, Joel and Michael McCauley (2008) http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

Mason, Richard O. 1986. "Four Ethical Issues of the Information Age." *Management Information Systems Quarterly* 10(1): 5-12

Schneier, Bruce. 2001. "Protecting Privacy and Liberty—The Events of 11 September Offer a Rare Chance to Rethink Public Security." *Nature* 413(Oct):773

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *Management Information Systems Quarterly* 20(2):167-196

Taylor, Humphrey. 2003. "Most People are 'Privacy Pragmatists' Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits." *The Harris Poll©* 17(March)

ABOUT THE AUTHOR:

Nicole L. Beebe, Ph.D., CISSP, is an assistant professor at the University of Texas at San Antonio's [UTSA] Department of Information Systems & Technology Management in the College of Business.
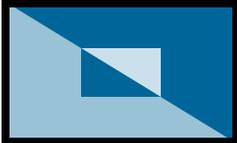
Security vs. Privacy:
Top 10 Things to Make Sure Your Home Computer Doesn't Get "Owned" by a Chinese Hacker Gang

By John B. Dickson, CISSP
Principal, Denim Group, Ltd.

Security blogger and ex-*Washington Post* reporter Brian Krebs experienced what many of us fear. His home computer, connected to the Internet, was attacked and taken over by a hacker. Not any hacker, name you, but an actual Chinese hacker gang. This experience opened Brian's eyes about the need to protect his computer, identity, private information, and ultimately his reputation from compromise. It also inspired Brian to become a deeper thinker about the larger question of computer security.

Why do normal users at home or work do things that make them likely targets? Is there a reasonable approach to securing your computer and your person information on it? Are we fated to be always at the mercy of hackers who will always be smarter and one step ahead of us? Can non-IT or non-security professionals really protect themselves?

The answer simply is "yes." There are a handful of reasonable things you can do to protect yourself from viruses, malware, attackers, and, yes, Chinese hacker gangs. There is an implied incentive – if you follow several easy steps, you can save countless hours of time or dollars trying to recover your computer, or worse yet, recover your identity if hackers steal your private information. **These simple, repeatable strategies include (in no particularly order):**

- Update computer operating systems: Those nagging Windows or Apple messages to update your computer with the latest patch or update are important and should be heeded. If your operating system is out of date, you are essentially vulnerable to attack by hackers who have devised a way to exploit your system. Considering turning you update program to "Automatic" mode so this happens without your conscience intervention.

- Update your anti-virus signatures regularly: Hackers are always trying to stay one step ahead by exploiting bugs in software; anti-virus companies are always updating their software to catch these new exploits. It's a cat and mouse game - if your anti-virus software is out of date, you are essentially unprotected.

- Update other programs on your computer as needed: In addition to your operating system and antivirus first lines of defense, you need to update/patch all the other software components on your system when prompted for the reasons outline above in #1 and #2.

- Don't mindlessly click through to unknown or untrusted web links: "Phishing" attacks happen when bad people send you a link to site that looks legit, but instead takes you to a server that will either try to harvest your username and password, or worse yet, download malware on your computer to wreak havoc. www.wellsfargo.biz is not www.wellsfargo.com!

- Never respond to an e-mail asking you to confirm your login credentials: This is a variation of step #4. If you did not initiate service from your bank, it's likely that your bank did not send you an e-mail to confirm your login information. These e-mails look very convincing and many times use logos and pictures consistent with the branding of the company they are attempting to mimic. Don't ever confirm sensitive account information via an e-mail sent to you without some type of initiating event on your side.
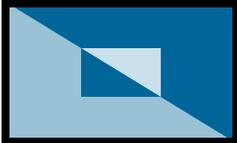
Security vs. Privacy:
Top 10 Things to Make Sure Your Home Computer Doesn't Get "Owned" by a Chinese Hacker Gang

- Make sure your wireless access point at home is locked down: One avenue of approach for local attackers is to hop on to an unprotected wireless access point broadcasting throughout the neighborhood (e.g., "Linksys").   Although an attacker has to be near your wireless device to conduct this attack, you don't want a bad guy doing things like initiating a spam or attacking others from a device that appears to come from your home.

- Don't reuse passwords: Don't use the same username and password combination for your Facebook, online banking, e-mail, and other personal or business accounts. If a hacker steals one password, you don't want every account you have online to be at risk. Vary usernames, and never use the same passwords if possible.

- Don't use weak or easily guessable passwords: In addition to not reusing your usernames and passwords for every online account you have, make sure to use strong passwords that are not easily guessable. Preferably don't use dictionary words as your password – they are easily broken by sophisticated password "cracking" applications. Also, don't use semi-public information such as your high school graduation date or your pet's name.   Hackers have been known to harvest this information on social networking sites, then direct intelligent password guessing attacks to gain entry to accounts.

- Stay away from the red light district of the Internet: Moral issues aside, there are solid technical reasons why to avoid the seedier sites on the Internet. Specifically, many of these sites publish "free" content in order to get listed on search engines and to draw you in. Once on their site, many attempt to download malware or do other nasty things to your computer.

- If something looks weird, it just might be: Trust your intuition. If anything doesn't appear to be genuine, or your intuition tells you that an incoming e-mail doesn't appear to be from your friend, there's a chance it might not be. You might do all the technical steps detailed above, and still be susceptible to a very sophisticated piece of malware. Your intuition is your last line of defense.

The list above represents a solid set of practices that will protect you from many of the threats on the Internet. This list is by no means exhaustive and threats evolve. There are tons and tons of other things you can do. But if you do these things, you are pointed in the right direction. This is a start of what I hope is a lifelong habit of awareness and protection that will encourage those wily Chinese hacker gangs to target someone else's home computer – not yours!

ABOUT THE AUTHOR:

John Dickson is a principal at Denim Group, Ltd. and a Certified Information Systems Security Professional (CISSP) whose technical background includes hands-on experience with application security, intrusion detection systems and telephony security. He helps Chief Security Officers of Fortune 500 and Federal organizations launch software initiatives and has served as Chief Information Security Officer for a major healthcare organization.