SAFE SPACES
in Cyberspace

UNIVERSITY OF CALGARY

Contents

Staying safe in cyberspace

The Internet has completely transformed the way we live our lives. It has also transformed our definition of the term ‘personal security.’

“If you’re connected then you are accepting risk,” says Rei Safavi-Neini, AITF Strategic Chair in Information Security, computer science professor in the Faculty of Science and Director of Institute for Security, Privacy and Information Assurance (ISPIA) at the University of Calgary. “A famous quote by FBI’s Dennis Hughes is: ‘The only secure computer is one that’s unplugged, locked in a safe, and buried 20 feet under the ground in a secret location… and I’m not even too sure about that one.’”

If you really like the convenience of shopping online, you are deciding to give the retailer personal information and your shopping preferences. If you like watching cat videos on Facebook, you are telling the social media site about your interests. “No one can stay private,” Safavi-Neini. “It is a series of decisions that you make every time you go on the Internet. If you want to access something, you reveal something.”

Understanding how those decisions are made is important for your own safety and security, says Tom Keenan, a professor in the Faculty of Environmental Design, adjunct professor in the Department of Computer Science at the University of Calgary and a research fellow at Canadian Global Affairs Institute.

“You can do things to help throw the bad guys off your digital trail,” says Keenan, who is also the author of a book on staying safe online: Technocreep: The Surrender of Privacy and the Capitalization of Intimacy.

FACTS

In 2015...

more than
430 million
new pieces of malware were created

Spear-phishing campaigns targeting employees increased **55%**

Over
half a billion
personal records were stolen or lost

Ransomware attacks grew
35%

Source: 2016 Internet Security Threat Report from Symantec

Tom Keenan's **10 tips** for staying safe online:

1 **Be a super skeptic.** You didn't win $10M in a lottery that you never entered, and Bill Gates or a man in Africa are not waiting to give you free money. Instead, their emails are often booby-trapped to infect your computer.

2 **Beware of ransomware**, malware that gets into your computer and encrypts your files, holding them hostage until you pay money. A hospital in California paid over US$17,000 recently to get their files back, and a wine store owner in Calgary paid US$500 to regain access to his inventory files and customers lists. Protect yourself from accidents and bad guys by having good backup copies of your photos, documents, and family videos.

3 **Watch your kids** because they can be too trusting in sharing photos and information. Have a good talk with them about setting limits.

4 **Help seniors** avoid Internet scams that target their banking and credit card information. Some have even lost their homes to scammers.

5 **Keep your software up-to-date.** This includes having good anti-virus and anti-malware protection.

6 **Be info-stingy.** While your bank and your employer might need your true date of birth, Facebook and other commercial sites don't need it. You should have a fake birthday for them. Your real "friends" will understand.

7 **Use strong passwords.** Far too many people use “12345” or “password” and also use the same password on different sites, which is a no-no. If you’re having trouble keeping track, there are password manager programs that can help.

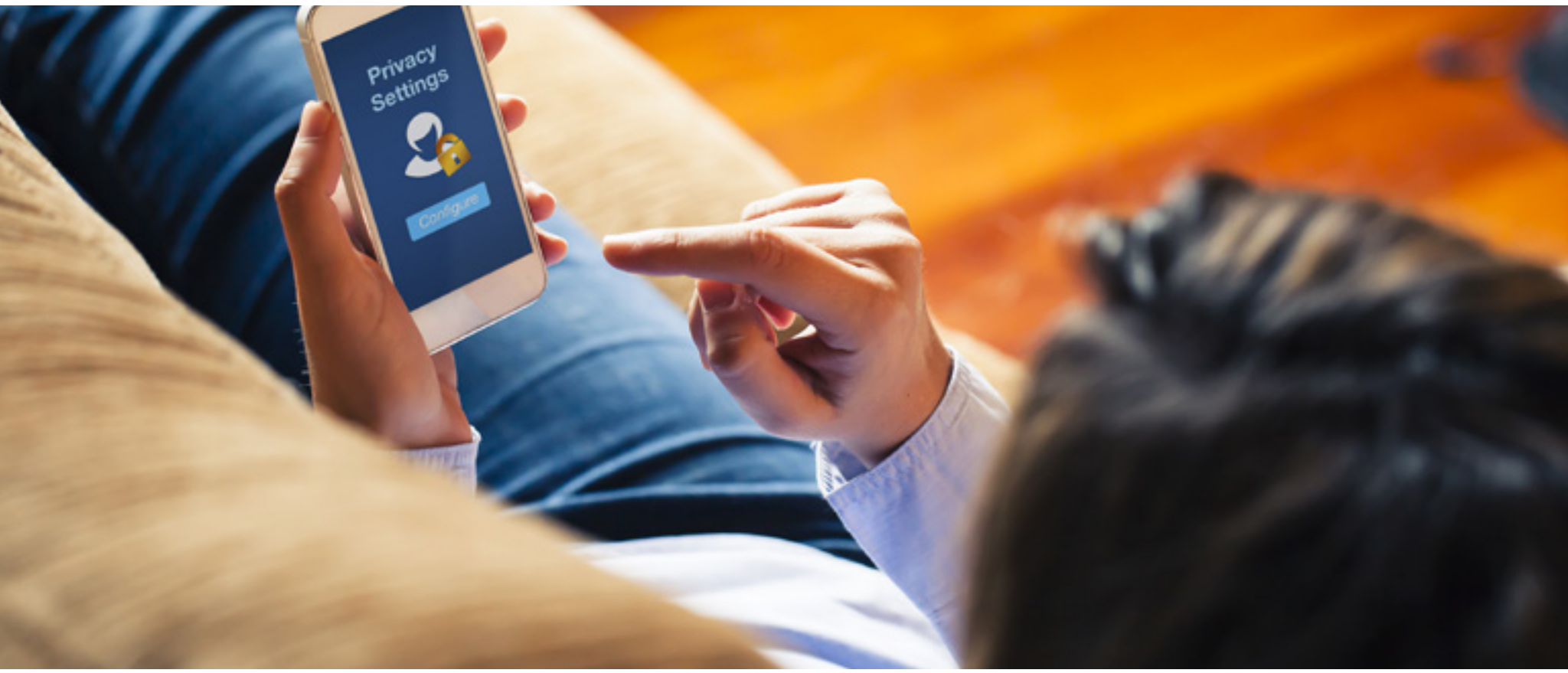
8 **Beware of phone scammers.** Not all the bad guys come in through your computer. If a caller says they are from your bank, credit card company, or the Canada Revenue Agency, hang up and call them to see if they really need to talk with you.

9 **Guard your bio-data.** While it sounds a little futuristic, that DNA sample you send off for analysis to determine your genetic makeup might someday come back to haunt you. It’s a good idea to keep this type of information separate from your real identity. Get one of those prepaid credit cards and use a fake name.

10 **Keep up on new vulnerabilities.** Every summer, new risks are unveiled at the hacker conferences like DEFCON and Black Hat. Recent ones included everything from the Nest thermostat, which can be hacked, to the Jeep Grand Cherokee, which can be taken over remotely while you are driving.

It is critical to be conscious of the information you share online or through your phone. Once a photo or a tweet is out there, you cannot control what happens next and it can be incredibly difficult to distance yourself from a controversial photo or tweet. Research in this area is incredibly important because we are still trying to understand how technology has changed the way people communicate, particularly youth, and the impacts of these changes.

Allyson Cairns-Walji, student Faculty of Law, University of Calgary



Don’t just dial it in:

Staying safe on your phone

Losing or having your phone stolen — along with all your personal information — is just one of many risks to watch for with your mobile phone. Here are some others:

- Be careful of Bluetooth transfers or attachments to text messages.
- Getting a text that asks you to call a number or write an email to ‘verify account information.’
- Do not install apps that ask for an unusual amount of your information.
- Unsecure WiFi can hand over your contact list and let someone else tap into your data plan. Your 3G connection is safer.
- Ignore prompts from companies you don’t know asking you to update, install or run software.

- Delete text messages you don’t recognize. They could be malware.
- Your phone may have been hacked if you receive charges you don’t recognize.
- Your sent folder has emails or texts you didn’t send.
- Your phone’s appearance or user interface has changed.

Source: Government of Canada

No one can stay private. It is a series of decisions that you make every time you go on the Internet. If you want to access something, you reveal something.

Rei Safavi-Neini, AITF Strategic Chair in Information Security, computer science professor in the Faculty of Science and director of Institute for Security, Privacy and Information Assurance (ISPIA) at the University of Calgary.