Cyber security Q&A: How to improve your online safety

By Andre Mayer, [CBC News](#)
Posted: Oct 3, 2011 3:14 PM ET
Last Updated: Oct 4, 2011 9:40 AM ET
  [Accessibility Links](#)

Beginning of Story Content

The federal government launched Get Cyber Safe on Oct. 3, a month-long push to improve Canadians' awareness of online security threats and of the steps they can take to protect themselves.

The public-service campaign includes a radio spot about choosing secure passwords and a video ad about deleting malevolent emails, and is tethered to a fairly comprehensive website.

In addition to raising awareness among the Canadian populace about bad surfing habits, the government is enhancing its own net safety in light of a massive attack on the Treasury Board and Finance Canada websites in February.

CBC News spoke to Toronto-based cyber security expert Dave Lewis, who has worked with a number of Canadian tech companies, runs Liquid Matrix, a blog about net safety matters, and is on the advisory board of the Security Education Conference Toronto (SECTOR), which runs Oct. 17-19. He offers insights into the latest online threats, as well as tips on how to avoid them.

CBC News: What are the most ubiquitous threats to individual users?

Dave Lewis: I would say the most ubiquitous threat to users is users themselves.

I know that may sound rather flippant, but users are their own worst enemies. They'll get an email that says "I love you" and they'll say, "Oh, how nice," and they'll click on the link without asking, "OK, why is this person sending me an email saying 'I love you?'"

Because we need that validation every day!

Yes, which is why the scammers and virus writers play on that regularly.

Besides the users themselves, what are the most ubiquitous threats?

The kinds of attacks that you see going through social networks that are made to look like one thing, but are actually something else. On Twitter up until recently — I don't know if they fixed it yet — but you could make a link look like it actually is going somewhere else. It could look like it's going to CBC.ca, but it's actually going to BadGuy.com. I'm overgeneralizing, but there is a lot of that problem.

People are quite vulnerable via email, are they not?

The worst ones are when people get malicious links in emails, and if they click on them, they could have their bank accounts compromised, which is really a significant issue. It's sort of like death by a thousand cuts. You have all of these bank accounts being compromised, to the tune of $200 here, $300 there - not enough for a

major crime unit to jump in and take action. If you hit on one of these emails with a maliciously crafted link, the real unfortunate side is most of these users have no idea that something has happened to them until they get the bill later.

What are some of the newer techniques of compromising a user's computer?

Toronto-based cyber security expert Dave Lewis. Dave Lewis

There's a new one from an organization that's ostensibly based out of India that used to be called Comantra. This is an organization that used to be a Microsoft Gold partner, and Microsoft took away their Gold status because they were randomly calling people saying, "You have a virus on your computer, give us your login and password so we can fix it." They called me at home a couple of times. They tried this routine on me, and I strung them along for a couple of minutes and then gave them an earful.

The problem here is you're getting people trying to access your computer, and they're just social-engineering you to give up your information. Once they're in your computer, lord knows what they're doing – installing malicious back doors, stealing information.

How many cyber attacks start with such a phone call?

That one is actually pretty brash. I have not seen this one before; I'm sure they happen. Usually, it's the lazy man's way of sending out a couple million spam messages and you get the 10 per cent return. This is a new one for me. We've seen it where [U.S. internet security company] HBGary Federal was compromised that way – they were compromised [in 2010] by the group Anonymous simply calling in and saying, "Hi, can I get my password reset?"

Low-tech works more often than not. If you want to get somebody's password, people say, "Oh, you can compromise it this way, and this way and that way" – or you can just ask them for it nicely.

Are there attacks that don't involve email penetration or fake URLs?

Drive-by attacks: users can go to something that looks completely normal and legitimate.

CBSNews, probably about six months, got compromised and they started [inadvertently] serving up malicious software. All the user had to do was surf to the website and they were compromised. They had no idea that it happened.

There are penetration tools for doing testing on sites, like BeEF, the Browser Exploitation Framework — you can use a browser as a pivot point and you can launch attacks as the user, using the user's credentials. You

could map an internal network, and the user has absolutely no idea that it's happening.

Are there any other emerging threats?

I think the attacks will change month to month, year to year, but at the root of it, you're trying to get information or money. Information is the currency of the day.

Educating the end user will help a great deal, but it's a very, very long process. And there isn't much financial incentive for companies to do that. They'll say, "OK, it costs me this much to educate the user base, or we could just take the hit and absorb the cost."

Banking is a perfect example. They'll say you have to have a [relatively low-security] six-character password, and that's fine. Some banks have plenty of checks and balances on the back end, whereas other banks, it's held together with baling wire and duct tape.

How useful are public awareness campaigns?

Humans are what they are – they're creatures of habit. So you can keep bringing the message. It will get through to some. Some will listen, some will take it to heart.

Maybe you have to be compromised yourself to finally take steps to defend yourself.

Yeah. It's sort of like if somebody breaks into your house, you feel violated. If someone breaks into your internet banking, wipes out your account, you feel violated. You will never forget that lesson.

What are some easy steps to avoiding cyber crime?

The absolutely easiest step is to take a moment and think about what you're about to click. If you get an email and it says it's from your bank – does your bank send you emails? Are they actually going to ask for your password? Take a moment to sit there and think – is this really what it's supposing to be? A moment's pause helps.

Make sure you have up-to-date anti-virus, and firewall on your local desktop.

Make sure your system is patched and up-to-date [with the latest software or operating system updates]. A lot of people buy their computer from various Future Shops and what-have-you, take it home, set it up and never apply a patch. So what happens is there are hackers out there who are constantly testing these systems – either good hackers or bad hackers, depending on what you want to be – these vulnerabilities are discovered from time to time. The results of that are published or in the worst-case scenario, a worm or virus leveraging a vulnerability could come out. And if your system is not patched and up-to-date, your system could be compromised just by being attached to the internet. You should set your computer up to automatically patch — 95 per cent of the time that works just fine.

People have cable modems coming out the wazoo now. They have high-speed access to the internet, so a lot of times there's a direct line back to their computer if they're not set up properly. If you have a firewall on your system – Microsoft has it built in, Linux has it built in – enabling these firewalls, if they're not already enabled, that's a huge win right there.

Should you have a different password for every website or application you use?

Realistically, yes.

I'm going to say something that you won't hear a lot of people say: write your passwords down. When I say that, don't put it on a sticky note and put it in your monitor. I mean, write it down on a sheet of paper, stick it in a safe or your safety-deposit box. Realistically, you should change them on a regular basis, but people aren't always going to remember their passwords.

Another thing they can do is use software like 1Password, which is an excellent password-encrypted container that will save all your passwords for you. You're keeping a record, but keeping a record that is safe and they're locked somewhere securely, so it's not a case of the cleaning lady walking through your house and saying, 'Ah, I'm taking this with me.'

Accessibility Links

Story Social Media

Related News Content

Stay Connected with CBC News

- Mobile
- Facebook
- Podcasts
- Twitter
- Alerts
- Newsletter

Big Box Advertisement

Top News Headlines

Tributes pour in for Apple's Steve Jobs
> Colleagues, competitors and world leaders are paying their respects to technology visionary Steve Jobs, who died Wednesday. more »

Energy drink labels to contain warnings
> Federal Health Minister Leona Aglukkaq has announced new rules for caffeine drinks such as Red Bull and Monster, but sales to minors won't be banned. more »

7 key races to watch as Ontario votes
> Polls in Ontario's heated provincial election close today at 9 p.m. ET. Here's a look at some of the more

interesting races to watch when the results start rolling in. more »

UN raises death toll in Syria unrest to 2,900
>   The UN's human rights office has raised its tally of people killed during seven months of unrest in
>   Syria to over 2,900. more »

Nobel Peace Prize loose lips fuel speculation
>   Speculation ahead of the Nobel Peace Prize announcement on Friday is split between the Arab Spring
>   and the European Union after cryptic comments by the award committee's chairman. more »

More Headlines »

Most Recent

- Watch
- Listen

Show previous slide
Show next slide

Latest Canada News Headlines

Energy drink labels to contain warnings
>   Federal Health Minister Leona Aglukkaq has announced new rules for caffeine drinks such as Red Bull
>   and Monster, but sales to minors won't be banned. more »

More storm surges to hit Maritimes
>   A storm that hit the East Coast Wednesday is expected to bring more storm surges Thursday afternoon.
>   more »

7 key races to watch as Ontario votes
>   Polls in Ontario's heated provincial election close today at 9 p.m. ET. Here's a look at some of the more
>   interesting races to watch when the results start rolling in. more »

Rescued sea lion released into wild
>   A California sea lion that was near death when it was rescued near Ucluelet, on the west coast of
>   Vancouver Island, in August has been released back into the wild. more »

Catholic order will pay Quebec abuse victims $18M
>   The Congregation of Holy Cross committed to issuing an apology and providing financial
>   compensation for abuses committed over 50 years at three institutions. more »

More Headlines »

On Tonight's National

Top stories

Tributes pour in for Apple's Steve Jobs

Keith Boag and Ron Charles
> Keith Boag looks at the tributes pouring in from colleagues, competitors and world leaders for technology visionary Steve Jobs, who died Wednesday. Ron Charles reports on the legacy of Steve Jobs and how Apple has changed the way we live our lives.

Ontarians head to the polls

Ioanna Roumeliotis
> Ontarians head to the polls today in Ontario's 40th provincial election. Liberal Leader Dalton McGuinty is seeking his third consecutive majority against opponents Tim Hudak of the Progressive Conservatives and the NDP's Andrea Horwath.

New energy drink rules expected

Kelly Crowe
> Federal Health Minister Leona Aglukkaq will be announcing new rules energy drinks this morning. She is concerned about teenagers and tweens consuming too much caffeine by downing drinks such as Monster and Red Bull.

See more stories from The National

The Current

- The Loss of Steve Jobs *Oct. 6, 2011 2:23 PM* Today on The Current, the loss of a man known for his I-deas. We look back at the forward vision of the late Steve Jobs.

Show previous slide

Don't Miss

ONTARIO VOTES CBC's election night coverage CBC offers multi-platform coverage throughout election night on Thursday

VOTE COMPASS CHART What issues matter most (and to whom)

Users of CBC's Vote Compass rate the issues of the Ontario election

Mom entrepreneurs Flexibility, boundaries key to melding parenting, business Running a business while raising young children is tricky but worthwhile

MOBILE PHONES Cellphones and health: precautions countries are taking Canada not alone in cautious approach to children's use of mobile phones

Natasha Fatah The problem with blackface

SMALL BUSINESS Comprehensive coverage of a key driver of Canada's economy News, trends and tips for Canadian entrepreneurs
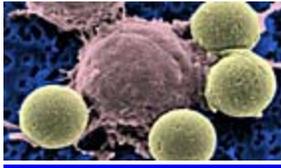
ENERGY A look at oilsands production from bitumen to barrel Canada's vast oil reserves have spurred critical debate

PROFILE Alison Redford, Alberta's next premier Tories elect new leader

FAQ Warrantless online spying or not? Clearing confusion about lawful access

MEDICAL RESEARCH Understanding immune system's choreography Nobel winners' work critical to ongoing studies

Copyright online What Copyright Act changes will mean for digital users Consumers get some protections but are hampered by digital locks

10 questions Test your news knowledge with the top story weekend quiz

Space travel Q & A with astronaut Chris Hadfield How he's training to command the space station

ONTARIO VOTES Where do the parties stand on key issues? The parties' positions on issues from healthcare to taxation

Joe Schlesinger Why can't we afford more straight talk on the economy?

CLIMATE CHANGE Report says climate change could cost Canada billions A look at some key conclusions

Show next slide