Caledon senior care experts offer senior cybersecurity

Canadians aged 65 and older represent the fastest growing group of internet users, according to Public Safety Canada.
But they do not always take the precautionary steps to stay safe online.
In fact, scammers will often target seniors because of perceived accumulated wealth, and they think that seniors are less likely to report crimes due to fear of embarrassment.
A new survey by Home Instead Inc., franchisor of the Home Instead Senior Care network of franchised businesses that provide in-home care services to seniors, found that two-thirds (64 per cent) of Canadian seniors have been the victim or target of at least one common online scam or hack. In addition, more than a third (39 per cent) report that someone has tried to scam them online, and 29 per cent of surveyed seniors have mistakenly downloaded a computer virus.
Mark Matz, director of policy and issues management with the National Cyber Security Directorate at Public Safety Canada, explained that encouraging seniors to safeguard themselves online can go a long way in protecting sensitive identity and financial information.
?Protecting yourself online is all about planning ahead,? he said. ?Seniors may never encounter a security breach online, but it's crucial to take the appropriate steps to ensure they don't become a target.?
To help seniors understand their risks online and take steps to protect themselves, the Home Instead Senior Care network collaborated with Public Safety Canada to launch a new public education program, Protect Seniors Online, available at www.ProtectSeniorsOnline.ca
The new program offers free resources and tips to help seniors understand how scammers operate, familiarize themselves with the most common senior scams and take proactive steps to help protect sensitive information. The resources include the online Can You Spot an Online Scam? quiz (http://dev.protectseniorsonline.com/quiz/) to test seniors' cyber security knowledge.
?For seniors, this is a time in their lives when they should be able to rest assured, trusting that their life's earnings are protected,? said Priscilla Fernandes of the Home Instead Senior Care office serving Caledon. ?Unfortunately, we know there are people who violate this trust. That is why we are committed to helping seniors empower themselves by understanding the ways they are at risk online and practising good cybersecurity habits to protect their information and reduce their chances of being scammed.?
Research shows that more and more seniors are going online ? and putting themselves at risk. According to Home Instead's survey, 96 per cent of aging adults use the internet at least once a week. They most commonly use the internet for email, with 93 per cent of seniors doing so weekly. Seniors also use the internet to manage finances, with 41 per cent banking online and just less than a quarter (21 per cent) paying bills online. Seniors are also active on social media, with 52 per cent using Facebook or Twitter at least once a week. All that time online ? coupled with what scammers view as perceived financial security and a trusting nature ? can make seniors a primary target for scammers.
Seniors are encouraged to take the following precautions, compiled by Public Safety Canada's Get Cyber Safe campaign (GetCyberSafe.ca), the Stop Think and Connect campaign and the Home Instead Senior Care network, to protect themselves online:
? Create passwords and make them strong. Lock all internet-enabled devices, including computers, tablets and smartphones, with secure passwords ? at least eight to 12 characters long and a mix of letters, numbers and symbols.
? Secure access to accounts, with two-step verification. Many online services, including apps and websites, offer free options to help protect personal information. Learn more at LockDownYourLogin.com
? Think before you act. Emails or messages that create a sense of urgency ? like a problem with a bank account or taxes ? are likely a scam. Reach out to companies by phone to determine if emails are legitimate.
? When in doubt, throw it out. If an email looks unusual, delete it. Clicking on links in email is often how scammers access personal information. Turn on spam filters to filter suspicious messages.
? Share with care. Be aware of what you share publicly on social media and adjust privacy settings to limit who can see your information.
? Use security software, including updated anti-virus and anti-spyware software.
? Adjust browser safety settings for optimum security.
? Use your computer's default firewall security protection on your computer.
? Log out. Log out of apps and websites when you're finished using them. Leaving them open on your computer or smartphone could make you vulnerable to security and privacy risks.
? Consider support. Seniors who live alone or spend a lot of time by themselves may want to consider a trusted source, such as adult family members, computer-savvy grandchildren, or professional caregivers, to serve as a second set of eyes and ears when

conducting activities online.

?Our hope is that by highlighting the ways scammers can gather sensitive information or hack technology, and providing seniors with cybersecurity solutions aging adults can implement themselves, we can help ensure their personal information, financial security and independence stay protected,? Fernandes said.

Seniors can test their cybersecurity skills at Can You Spot an Online Scam? at http://dev.protectseniorsonline.ca/quiz/ and view other program resources and tips atProtectSeniosOnline.ca

Or, contact a local Home Instead Senior Care office for additional resources and to learn how their professional CAREGiversSM may be able to assist. Find the nearest office by visiting www.homeinstead.ca/