Sensible Surfing

Kingston Diocesan Convention
May 4, 2014
Presented by Colleen Randall, 2nd Vice-President,
Ontario Provincial Communications Chair

We spend so much time these days online that we often forget about the old days…

When we sat around the wood stove in the kitchen and talked to friends and family. We shared stories, songs and laughter…

Pope Francis has said…

"We need to resolve our differences through forms of dialogue which help us grow in understanding and mutual respect. A culture of encounter demands that we be ready not only to give, but also to receive. Media can help us greatly in this, especially nowadays, when the networks of human communication have made unprecedented advances. The internet, in particular, offers immense possibilities for encounter and solidarity. This is something truly good, a gift from God."

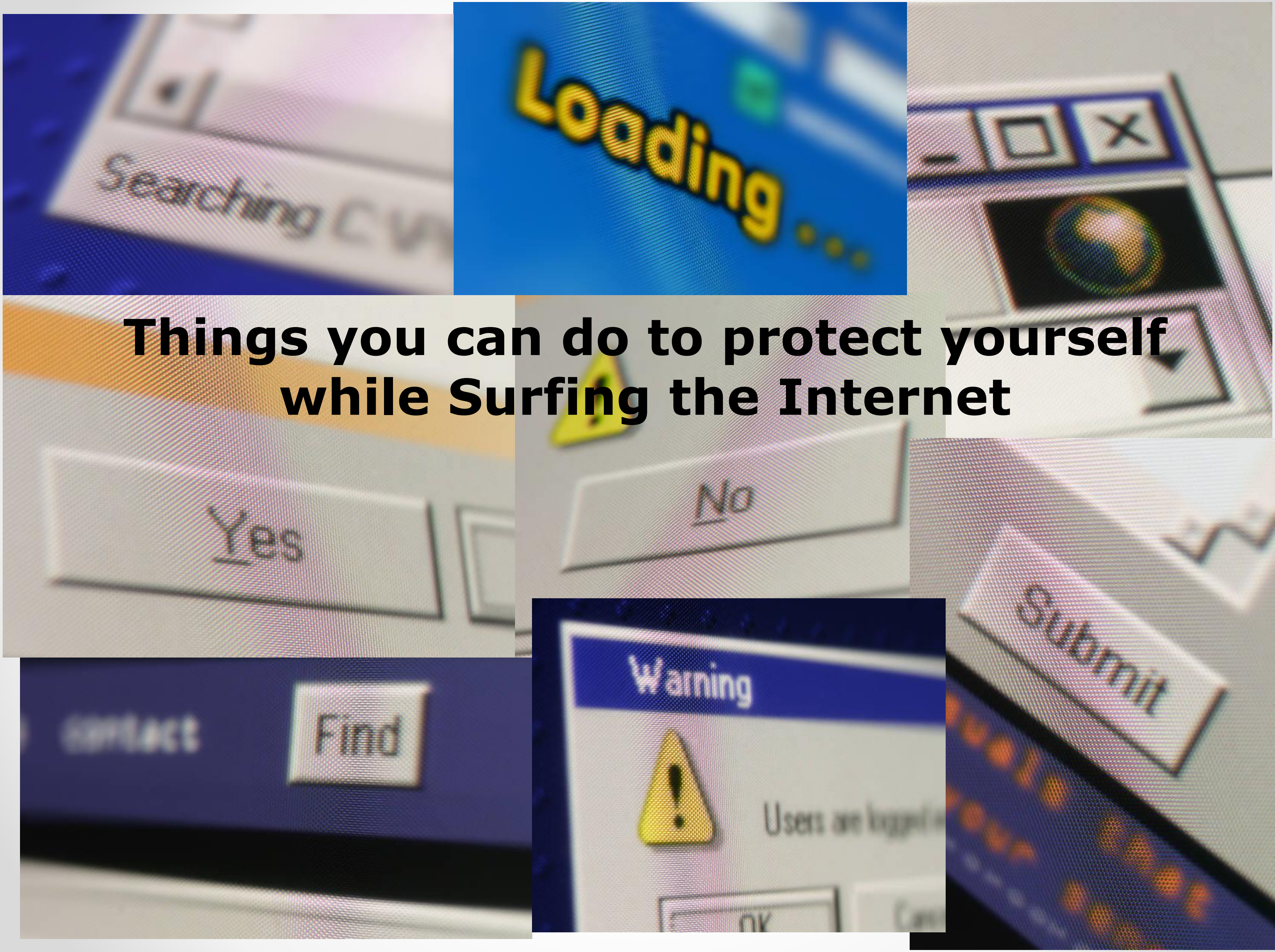
But … be warned…the web "can have the effect of isolating us from our neighbours, from those closest to us" and also reminded us not to "overlook the fact that those who for whatever reason lack access to social media run the risk of being left behind."

Email, Facebook, Twitter, Skype, Face time etc…

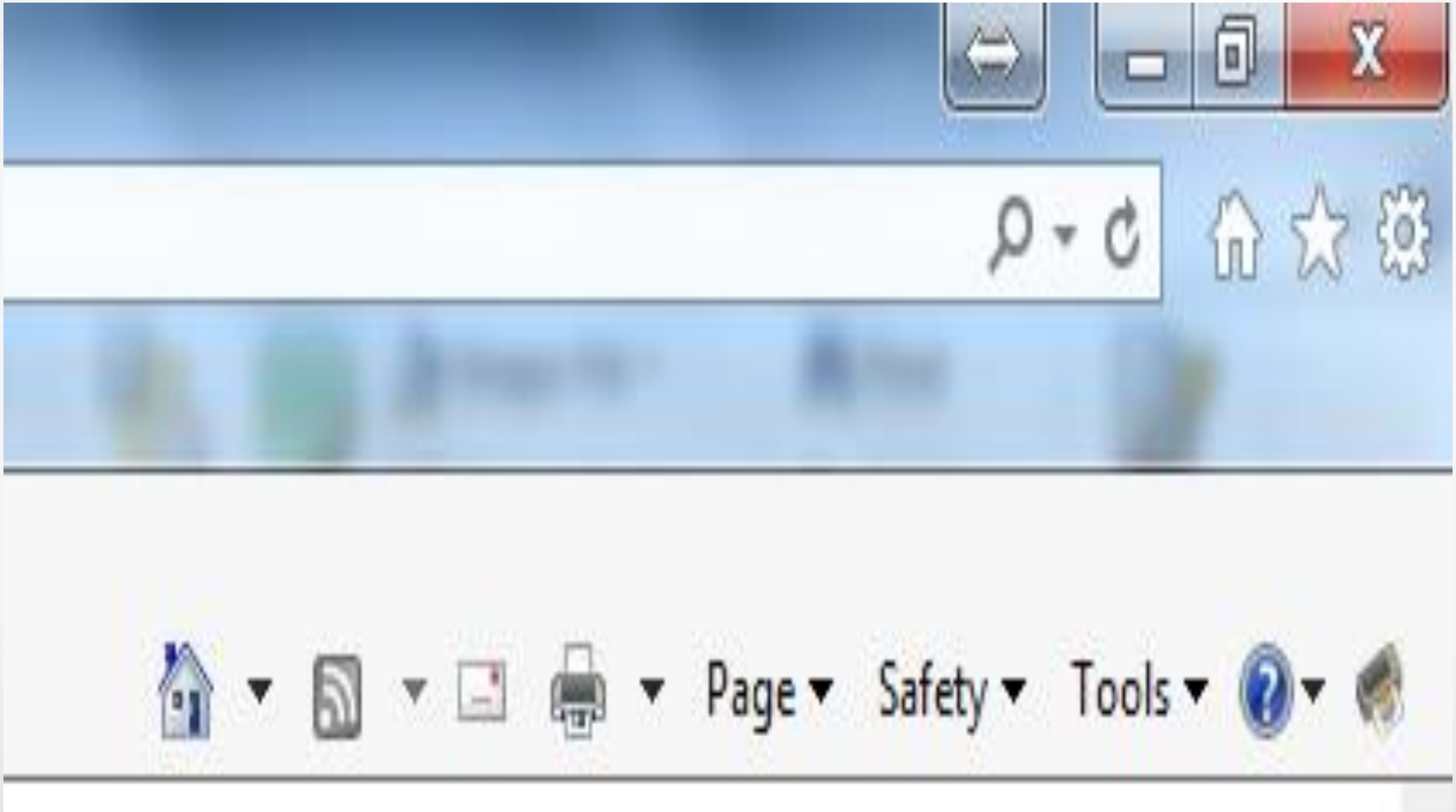
Has made our world so small…

Let's learn more about the tools of our evangelization…

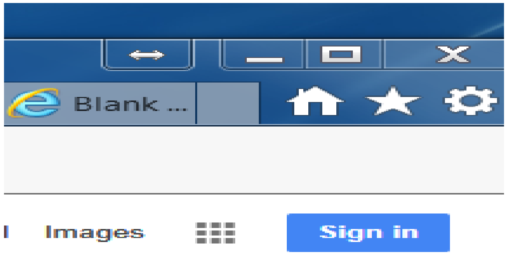
Things you can do to protect yourself while Surfing the Internet

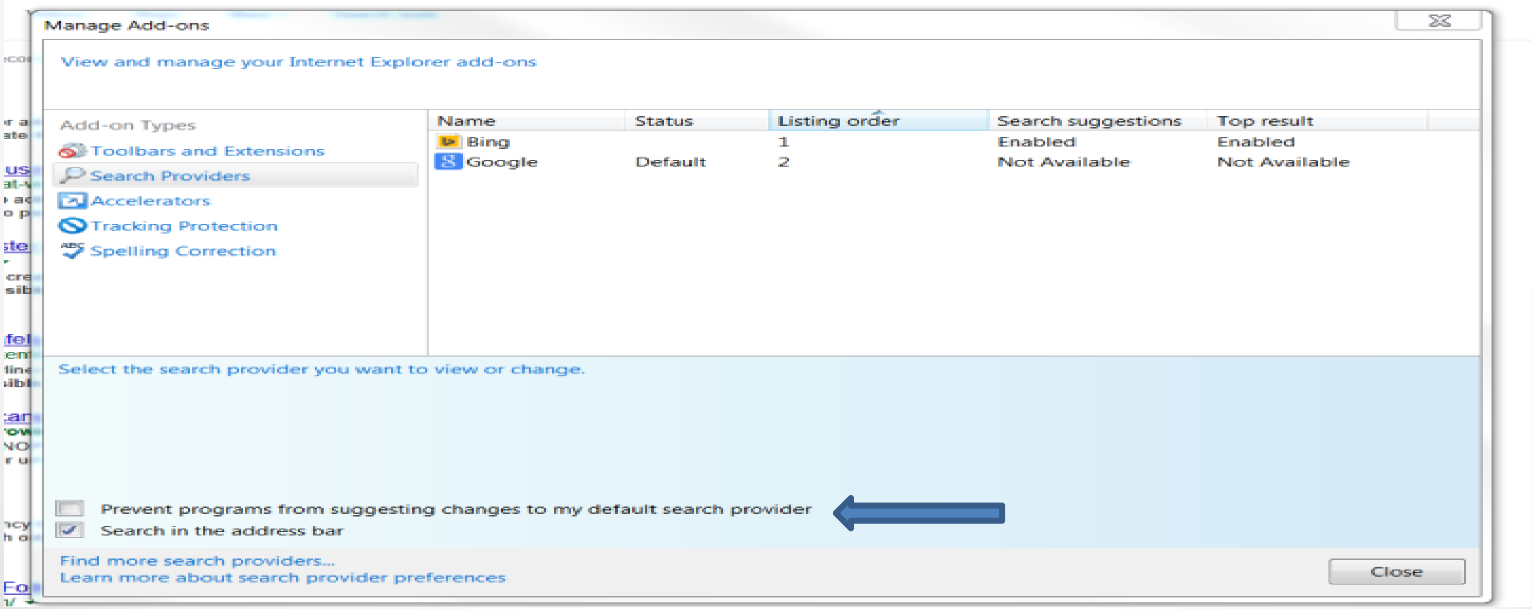


Get to know your “Tools”



In your browser, make sure the checkbox that **PREVENTS PROGRAMS from suggesting changes** to default search provider **is** Checked. (here it is not) Click on: Gear upper right corner: Then “manage ADD-Ons”




Manage Add-ons

View and manage your Internet Explorer add-ons

Add-on Types
- Toolbars and Extensions
- Search Providers
- Accelerators
- Tracking Protection
- Spelling Correction

Name	Status	Listing order	Search suggestions	Top result
Bing		1	Enabled	Enabled
Google	Default	2	Not Available	Not Available

Select the search provider you want to view or change.

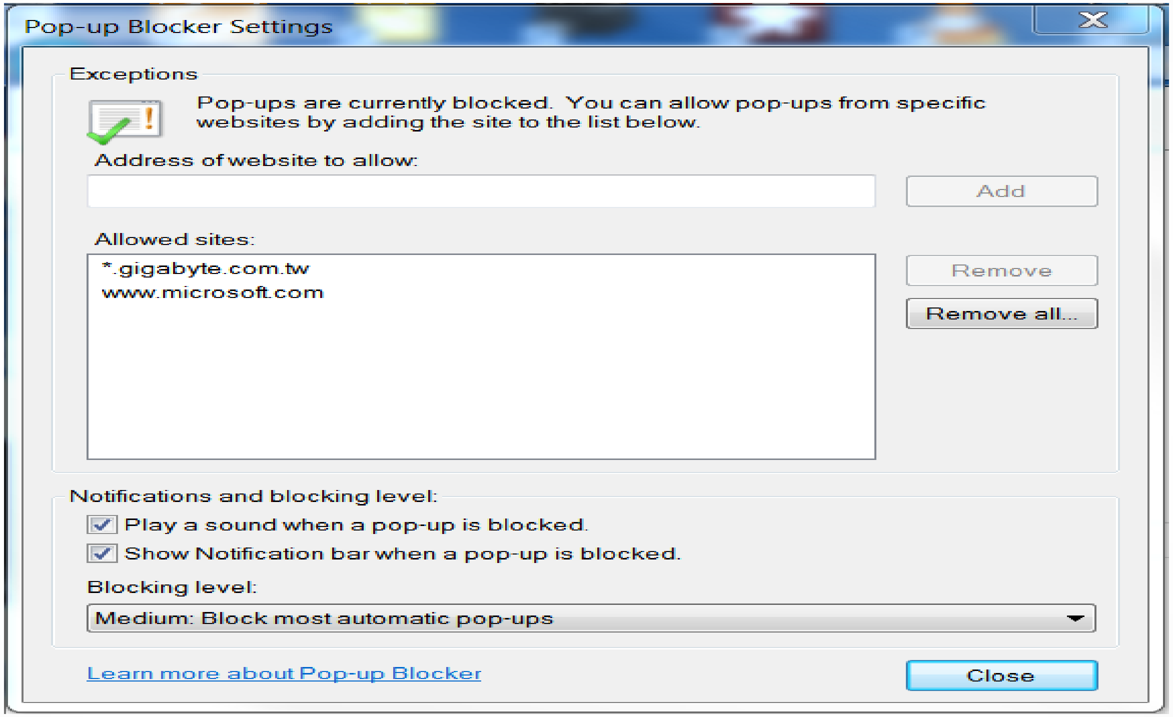
□ Prevent programs from suggesting changes to my default search provider

☑ Search in the address bar

Find more search providers...
Learn more about search provider preferences

Pop-up Blocker

Ensure your POP-UP BLOCKER is turned on. Click: TOOLS/Pop-up Blocker/Popup Blocker Settings;



Pop-up Blocker Settings
Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow:

Allowed sites:

*.gigabyte.com.tw
www.microsoft.com

Remove
Remove all...
Notifications and blocking level:

☑ Play a sound when a pop-up is blocked.

☑ Show Notification bar when a pop-up is blocked.

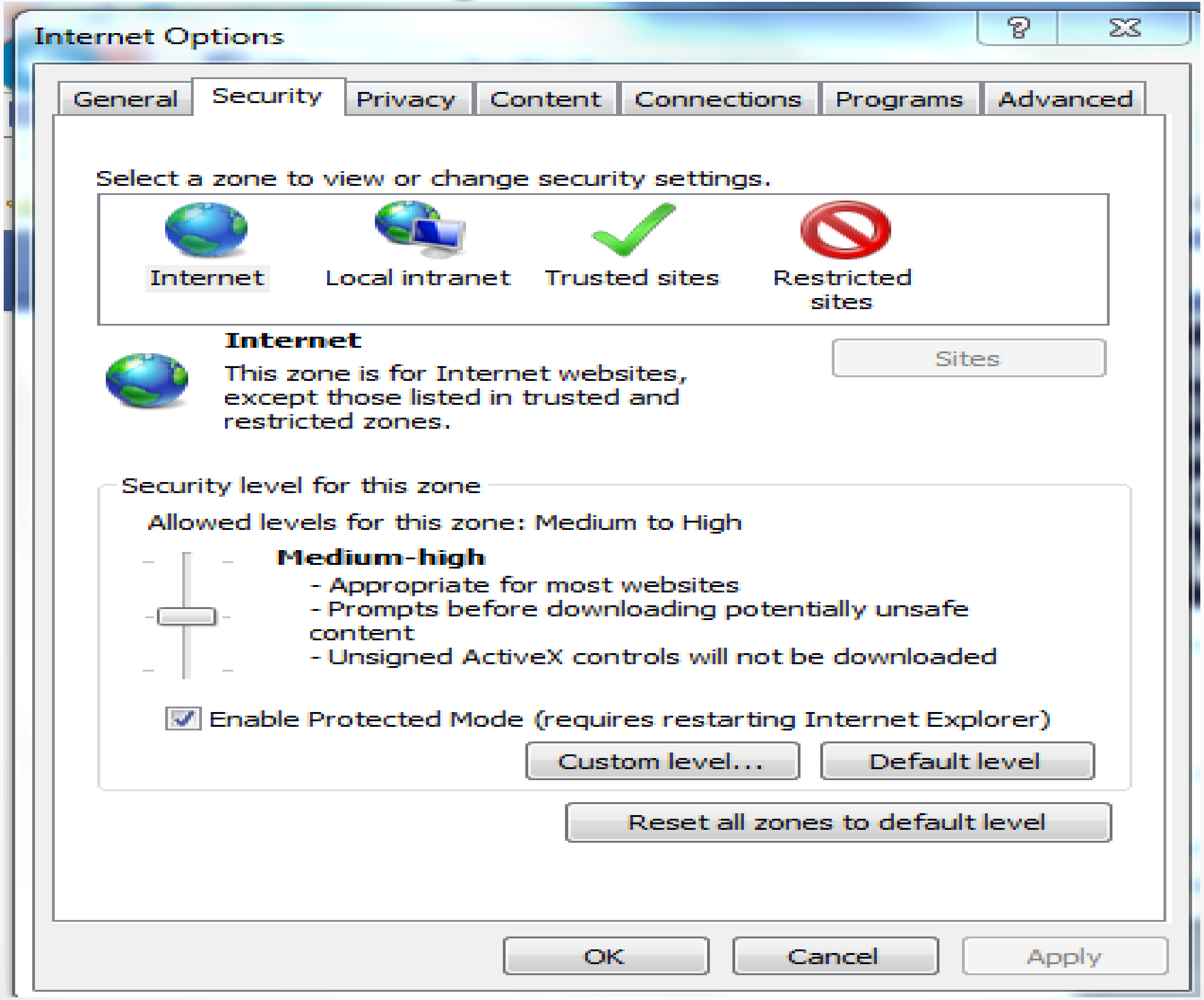
Blocking level:

Medium: Block most automatic pop-ups

Learn more about Pop-up Blocker
Close

Add the complete URL (http://etc.com) then click *Add* for the site you COMPLETELY trust

Internet Options - Security



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

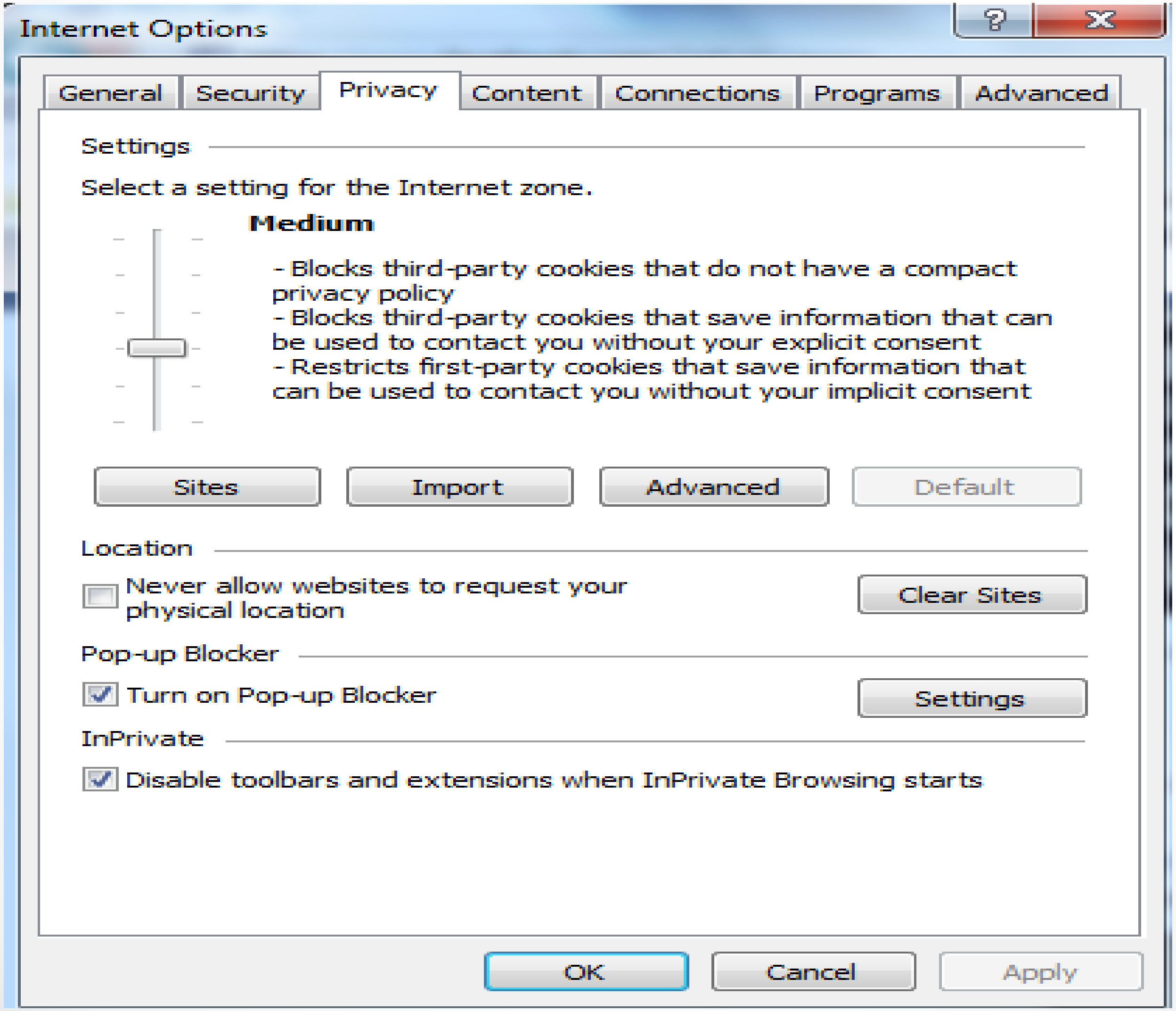
Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Internet Options - Privacy



Internet Options

Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Location

□ Never allow websites to request your physical location

Pop-up Blocker

☑ Turn on Pop-up Blocker

InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

Now that you know your computer…

- When “searching” use your search engine of choice – I always use Google.
- Go to trusted results sites
- READ ALL PROMPTS THOROUGHLY AND COMPLETELY
- When in doubt quit or cancel your transactions

Protect yourself…

Antivirus Software (prevent viruses)

Free to use:

- **Microsoft Security Essentials**
  Download here:
  http://windows.microsoft.com/en-CA/windows/security-essentials-download
- **Avast! Free Antivirus**
  Download here:
  http://www.avast.com/en-au/free-antivirus-download
- **Avira AntiVir Personal Edition**
  Download here:
  http://www.avira.com/en/avira-free-antivirus

Purchased software (Google search: ANTIVIRUS SOFTWARE)

- **Norton Antivirus (Many variations)**
- **McAfee Antivirus(Many variations)**
- **Viper Antivirus**
- **AVG Antivirus**
- **Kaspersky Antivirus**
- **Bitdefender**

Malware

Malware (Virus removal)

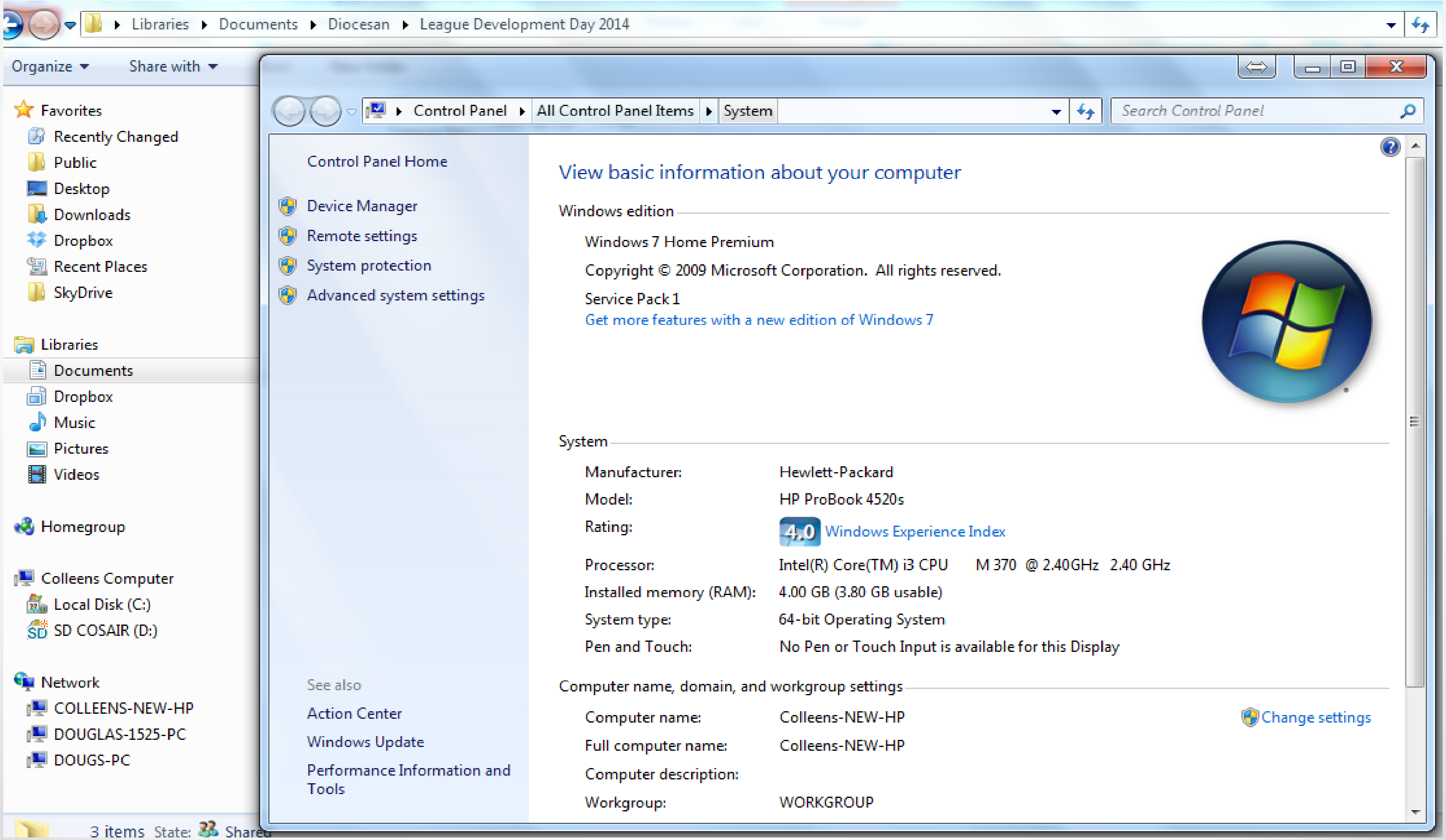
- Microsoft Malicious Software Removal Tool (a part of WINDOWS)
- Windows Defender Offline
  Download Here:
  http://windows.microsoft.com/en-ca/windows/what-is-windows-defender-offline (32 bit and 64 bit versions)
- Malware Anti-Malware
  Download Here:
  https://www.malwarebytes.org/free/ (there is also a paid version)

Resource for technical software:

- http://www.bleepingcomputer.com/

To check your own computer

- Right click on My Computer, Pick Properties



View basic information about your computer

Windows edition

Windows 7 Home Premium

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

Get more features with a new edition of Windows 7

System

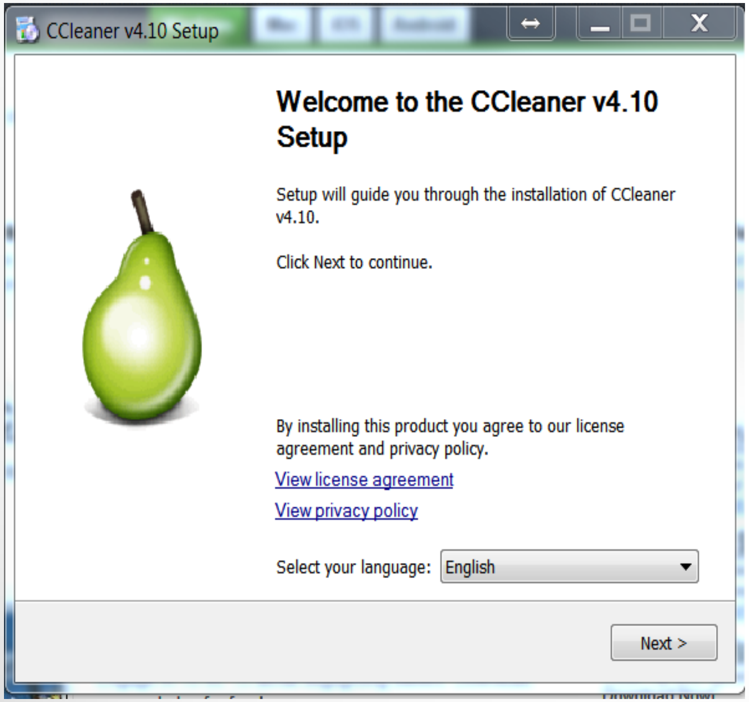
Manufacturer:	Hewlett-Packard
Model:	HP ProBook 4520s
Rating:	4.0 Windows Experience Index
Processor:	Intel(R) Core(TM) i3 CPU M 370 @ 2.40GHz 2.40 GHz
Installed memory (RAM):	4.00 GB (3.80 GB usable)
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:	Colleens-NEW-HP
Full computer name:	Colleens-NEW-HP
Computer description:	
Workgroup:	WORKGROUP

When installing software…

- Be careful that unwanted “options/toolbars/(crap)” in not piggy-backed into the install software. READ carefully what the install software is saying.
- Often, on these subsequent screens, add-on products will be installed but you can avoid them by unchecking the appropriate boxes.



CCleaner v4.10 Setup

Welcome to the CCleaner v4.10 Setup

Setup will guide you through the installation of CCleaner v4.10.

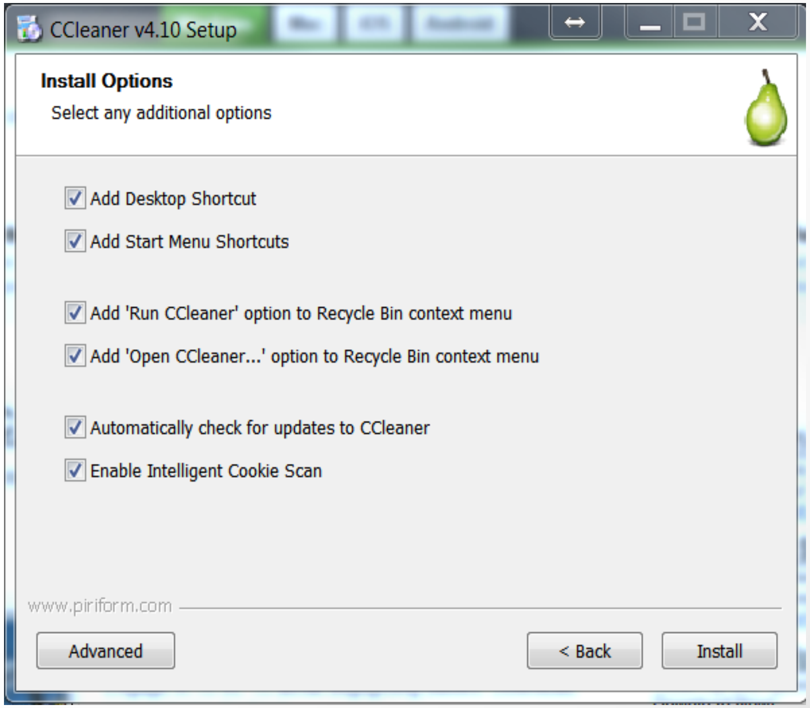
Click Next to continue.

By installing this product you agree to our license agreement and privacy policy.

View license agreement

View privacy policy

Select your language: English



CCleaner v4.10 Setup

Install Options

Select any additional options

☑ Add Desktop Shortcut

☑ Add Start Menu Shortcuts

☑ Add 'Run CCleaner' option to Recycle Bin context menu

☑ Add 'Open CCleaner...' option to Recycle Bin context menu

☑ Automatically check for updates to CCleaner

☑ Enable Intelligent Cookie Scan

If you make a mistake…

- Use **SYSTEM RESTORE**. One of the best forgotten tools. System restore will put your computer back to the way it was, BEFORE you installed the program. AND it does not cause you to lose ANY of your files. Just enter SYSTEM RESTORE on the PROGRAM SEARCH LINE, (use the WINDOWS KEY, then just type) You will get a list of dates that the computer took a “snapshot” of the computer settings, select the one you need and wait until it restarts. It will be as if you never installed the programs. (NOTE: Any WINDOWS updates will need to be redone.)
- SYSTEM RESTORE only works on programs and will not affect your documents

Your last line of defense…

A good technician is a definite asset…

The guys from Microsoft will **NEVER** call you to say you have a virus on your computer…

NEVER EVER allow a stranger to remotely access your computer…

Questions

???

Keeping your child safe on the internet

- **Step into their world…**

Be involved! Be an active participant in their surfing

- **Set house rules…**

You decide how much time they spend online and which sites they may go to. Post a list beside the computer. If they want to surf anywhere else they need your permission.

Keeping your child safe on the internet

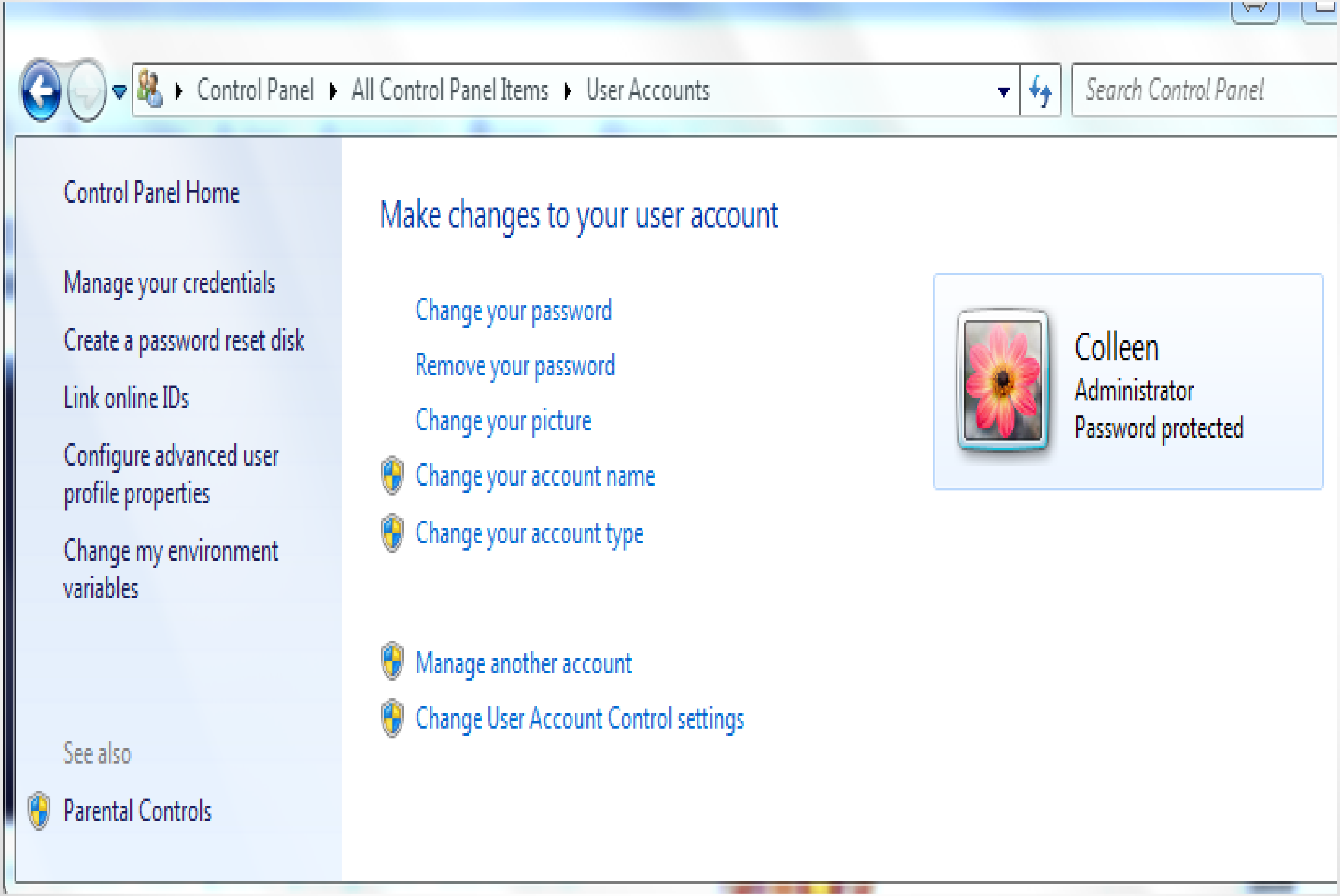
- **Teach them to protect their privacy**
  - never to give their name, phone number, e-mail address, password, postal address, school, or picture without your permission
  - not to open e-mail from people they don't know
  - not to respond to hurtful or disturbing messages
  - not to get together with anyone they "meet" online.

More Tips to keep the kids safe…

- **Know that location is the key…** keep the computer in a location where it is easy to monitor its use. The most popular location suggested by my research is in the kitchen. It is very open and the environment encourages conversation while your child is on the internet.

- **Be their go-to person…** let them know that the moment they are uncomfortable with a situation or interaction on the computer they should come to you, without blame or loss of privileges.

Use parental controls on your browser



Control Panel ▸ All Control Panel Items ▸ User Accounts

Search Control Panel

Control Panel Home

Manage your credentials

Create a password reset disk

Link online IDs

Configure advanced user profile properties

Change my environment variables

See also

Parental Controls

Make changes to your user account

Change your password

Remove your password

Change your picture

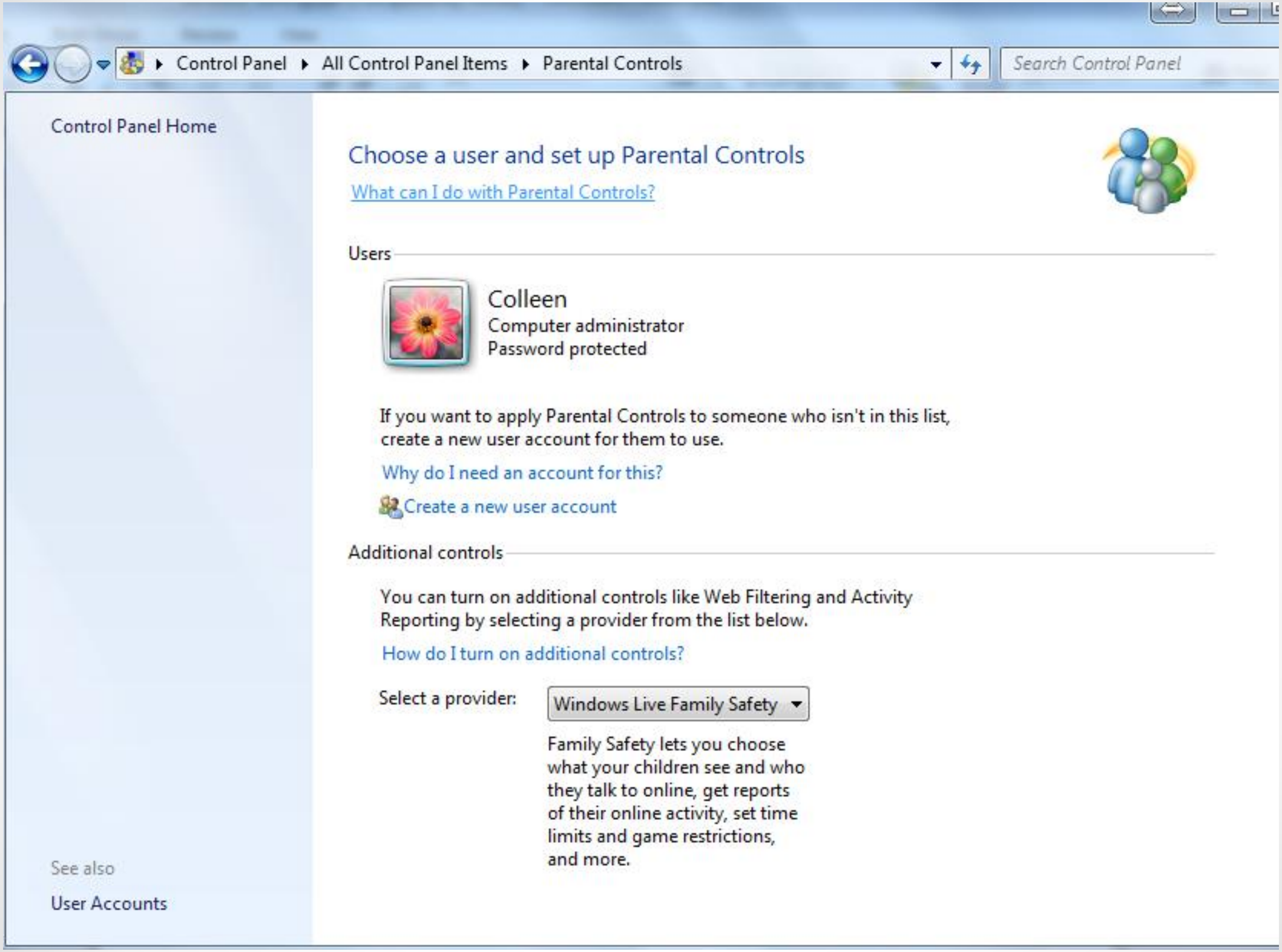
Change your account name

Change your account type

Manage another account

Change User Account Control settings

Colleen
Administrator
Password protected



Choose a user and set up Parental Controls

What can I do with Parental Controls?

Users

Colleen
Computer administrator
Password protected

If you want to apply Parental Controls to someone who isn't in this list, create a new user account for them to use.

Why do I need an account for this?

Create a new user account

Additional controls

You can turn on additional controls like Web Filtering and Activity Reporting by selecting a provider from the list below.

How do I turn on additional controls?

Select a provider: Windows Live Family Safety

Family Safety lets you choose what your children see and who they talk to online, get reports of their online activity, set time limits and game restrictions, and more.

- Be proactive
  - Children as young as 3 or 4 can search the internet these days
  - Do some research yourself – Google “Keep your kids safe on the internet” – there are lots of ideas there
  - There are a lot of tools available to you
  - Talk to your children
  - Let them know what is acceptable and what is not
  - Remember that one little typo in a search engine could be *disastrous*
    - Think of a 5 year old typing leg instead of lego

The following are recommended sites from Deacon Brent McLaren:

Here are Google's instructions for Safe Search:

https://support.google.com/websearch/answer/510?hl=en

You can also lock it on ... right there at the outset. You used to have options but now it is simply "Filter Explicit Results" and it is worthwhile turning it on. You mentioned "leg" ... some of the results for "Virgin Mary" can get really out there!

I also recommend KidRex (http://kidrex.org)

I get a lot of use out of a website called "DuckDuckGo.com" It is a secure site that does not track your searches or place cookies on the computer.

Questions

???

March was Fraud Prevention Month

Mobile phone scams are becoming increasingly common, especially malware targeting smartphones. Here are some threats to watch out for:

- **Missed call scams**: Scammers call your phone and hang up quickly. Your phone registers a missed call from a number you don’t recognize. If you call the number to find out who called you, you may end up paying a premium rate for the call without warning.
- **Text message scams:** Scammers send you a text message pretending to be someone you know (“Hi, it’s John. I’m back! When are you free to catch up?”) but from a number you don’t recognize. If you reply, you may be charged a premium rate for the message.

- **Ringtone scams:** Scammers send you an offer for a free or low-cost ringtone, but if you accept the offer you may unknowingly subscribe to a service that will keep sending you ringtones and charging you a premium rate each time.

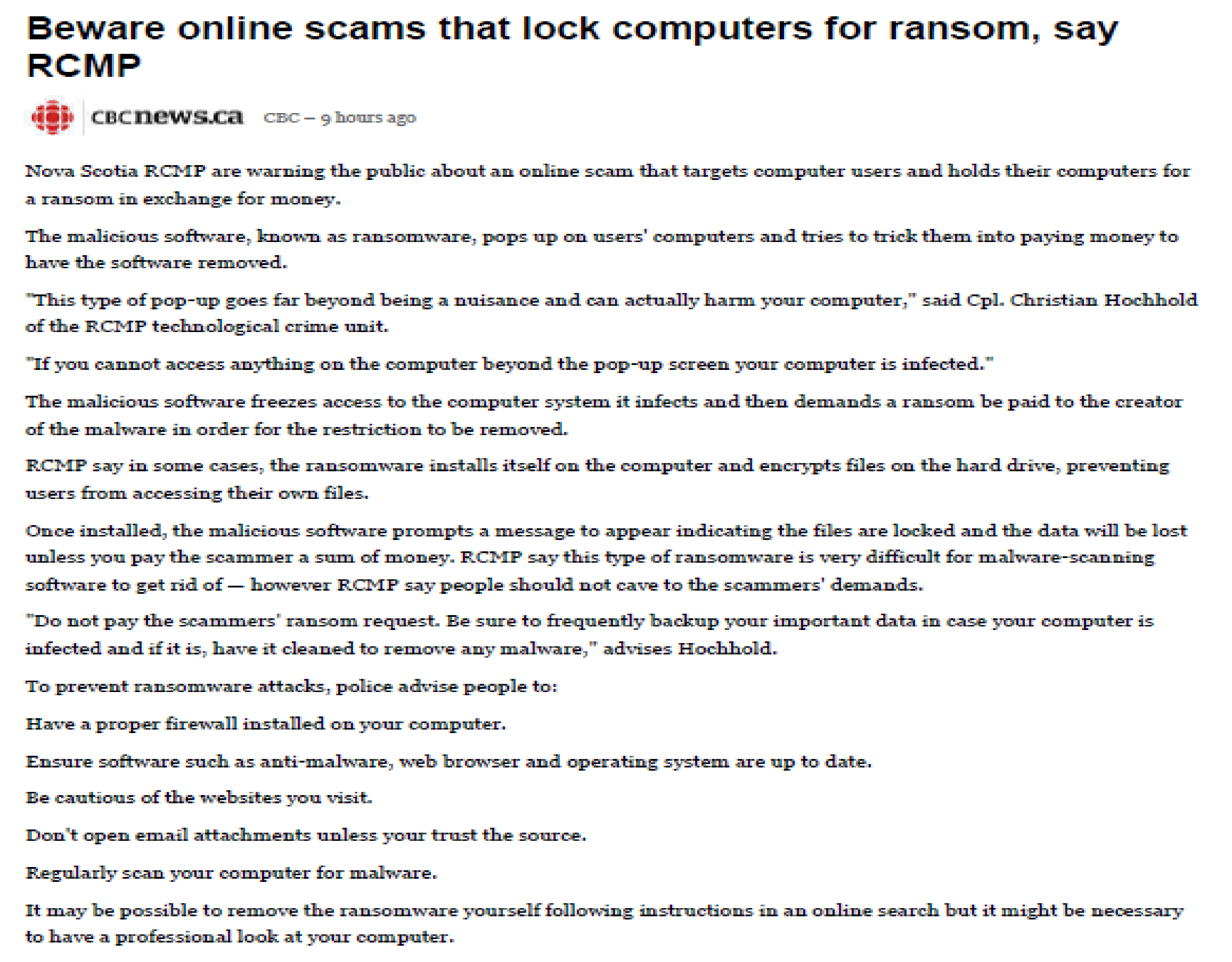
- **Malware:** Malicious software can be installed on your phone when you download disreputable apps or files, or if you visit unsecured websites. Often difficult to detect, malware lets criminals access your phone to disrupt its operation or steal your data.

Protect yourself

- Never reply to missed calls or text messages from numbers you do not recognize.
- Don't call or text phone numbers beginning with 1-900 unless you are aware of the cost involved.
- Read the terms and conditions of all offers very carefully. Services offering free or very cheap products often have hidden costs.
- Before downloading an app, do some research and see if it has been reviewed by a reputable source.
- Don't tamper with or "jailbreak" your smartphone's operating system. This will make it more vulnerable to malware.

Report it

- If you've been a target of a mobile phone scam, please call the Canadian Anti-Fraud Centre at 1-888-495-8501 or visit antifraudcentre-centreantifraude.ca.



Beware online scams that lock computers for ransom, say RCMP

CBCnews.ca CBC – 9 hours ago

Nova Scotia RCMP are warning the public about an online scam that targets computer users and holds their computers for a ransom in exchange for money.

The malicious software, known as ransomware, pops up on users' computers and tries to trick them into paying money to have the software removed.

"This type of pop-up goes far beyond being a nuisance and can actually harm your computer," said Cpl. Christian Hochhold of the RCMP technological crime unit.

"If you cannot access anything on the computer beyond the pop-up screen your computer is infected."

The malicious software freezes access to the computer system it infects and then demands a ransom be paid to the creator of the malware in order for the restriction to be removed.

RCMP say in some cases, the ransomware installs itself on the computer and encrypts files on the hard drive, preventing users from accessing their own files.

Once installed, the malicious software prompts a message to appear indicating the files are locked and the data will be lost unless you pay the scammer a sum of money. RCMP say this type of ransomware is very difficult for malware-scanning software to get rid of — however RCMP say people should not cave to the scammers' demands.

"Do not pay the scammers' ransom request. Be sure to frequently backup your important data in case your computer is infected and if it is, have it cleaned to remove any malware," advises Hochhold.

To prevent ransomware attacks, police advise people to:

Have a proper firewall installed on your computer.

Ensure software such as anti-malware, web browser and operating system are up to date.

Be cautious of the websites you visit.

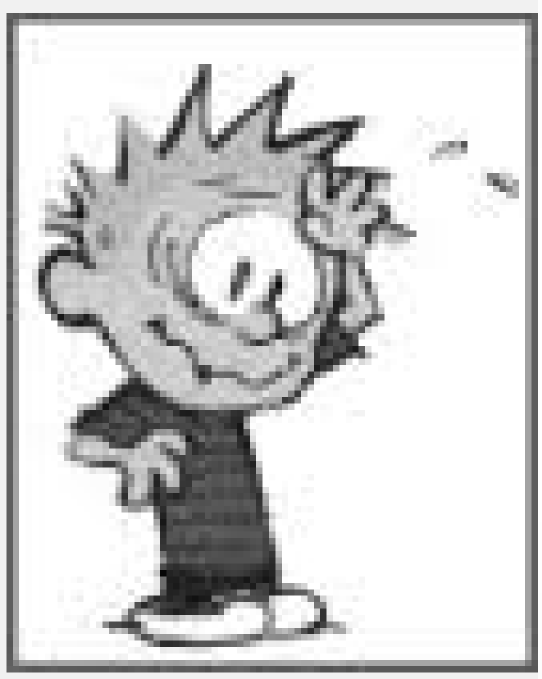
Don't open email attachments unless your trust the source.

Regularly scan your computer for malware.

It may be possible to remove the ransomware yourself following instructions in an online search but it might be necessary to have a professional look at your computer.

Questions

???



The final thoughts…

Knowing the Family

Our family was at a weekend getaway in the mountains, and when the power went out, I couldn't recharge my smart phone.

When the battery finally died, I couldn't Google, Facebook, email, Tweet, or look at pictures.

And no apps to play with. On top of that, it was raining. So ... we stayed in and I began to talk to my wife Sarah and our two children for a few hours.

***They seem like nice people*.**