Privacy Matters

A guide to help Canadians protect their online and offline privacy

Media Smarts

CANADIAN CENTRE *for* CHILD PROTECTION®
Helping families. Protecting children.

TELUS®

Privacy Matters

Welcome note from Andrea Goertz

The advent of online and mobile technologies and their fast adoption has resulted in our digital footprints growing exponentially. These technologies have provided us tremendous opportunities. We are now connected more than ever and have quick access to information that educates and entertains us. We are empowered and enabled to share our ideas and create our own space professionally and financially.

The Internet is ours and understanding the risks of participating in this online world is a shared responsibility.

Educating Canadians on how to keep their families and communities safer online, including online privacy, is something we take seriously at TELUS. This guide has been created as part of our TELUS WISE program – a unique educational program focused on Internet and smartphone safety that is available to all Canadians free-of-charge.

In order to create this guide, it was necessary to build on a solid understanding of what online life looks like for Canadian children. Our TELUS WISE partner, MediaSmarts, conducted research involving over 5000 Canadian kids (grades 4 through 11), with the results informing this guide. Additionally, the Canadian Centre for Child Protection and the Royal Canadian Mounted Police provided valuable information on steps we can take to protect our families online.

I would like to thank all of our partners for their contributions. I hope you find this guide as valuable as I have in helping our families, friends and communities be safer online.
Privacy matters.

Regards,

Andrea Goertz
Chief Communications and Sustainability Officer, TELUS Corporation

1. How connected are you?

Do you have these accounts?	Email	YES	NO
	Twitter	YES	NO
	Facebook	YES	NO
	Instagram	YES	NO
Do you text?		YES	NO
Do you download apps to use on your smartphone?		YES	NO
Do you shop or bank online? Do you share photos online?		YES	NO
Now add up how many email accounts, social networking accounts (e.g. Twitter, Facebook, Instagram), mobile apps, online banking and online shopping accounts you have? What does it add up to?			
Stop to think about how many Internet-enabled devices you and your family have. Include smartphones, computers/laptops, tablets, game councils and iPods. What does it add up to?			

Even if you just have an email account and only do general web surfing you are 'connected' and a member of our growing digital society. In the following sections of this guide we will share tips on how to protect your and your family's online privacy.

Protecting your information from others who might cause you harm is very important. We have many technologies to help with this, including virus protection, fire walls, back up programs, but they're only as good as their user, so it's critical that we keep ourselves up-to-date on the latest technology trends and ideas.

Did you know?

- Canada has the highest social media network penetration in the World. 82% of Canadian Internet users visit social networking sites in comparison to 75% of Americans.
- 46% of mobile phone users in Canada have a social media app.
- Canadians send more than 270 million text messages a day (source CWTA)
- More than 19 million Canadians are now logging onto Facebook at least once every month – that's more than half the population – while 14 million check their newsfeed every single day.

2. Defining online privacy

While the Internet is a wonderful medium to collaborate, communicate, connect and conduct commerce – we need to understand how to protect our family's, privacy.

What is online privacy?

As Canadians embrace social networks and other online technologies, they are sharing increasing amounts of personal information over the Internet.

Even with the toughest privacy settings, your online activities are never entirely private. Your clicks and website visits leave data trails. Over time, these coalesce into a highly informative digital shadow that reveals a lot about who you are, what you do, and what you like and dislike.

And that's valuable information. Businesses may use it to tailor ads to your interests or preferences. In extreme cases, criminals can find sophisticated ways to trick you into providing your financial and other sensitive personal information online to defraud you.

In other words, you may go online to network with friends. But, in the online world, you may not always be among friends.

Source: Office of the Privacy Commissioner of Canada.
https://www.priv.gc.ca/resource/topic-sujet/owp-pvplrsf/index_e.asp

In the next sections you will find some valuable tips on protecting your and your family's, online privacy.

3. Social networks and mobile application tips

Courtesy of TELUS WISE

Think about the social networking sites you, your kids, and your parents participate in (e.g. Twitter, YouTube, Facebook, Instagram). Also think about mobile applications that you download (e.g. weather, games, mapping applications).

It is really important that your permission and privacy settings on social networking accounts and apps that you download, are set to where you want them to be. You really need to pay attention to the privacy and permission terms and settings – just don't accept them blindly.

Permission settings

Permission settings control what can and cannot be accessed and shared about you (e.g. contact lists, computer files including photos, and your profile) by a social networking site or mobile app that you subscribe to.

Privacy settings

Privacy settings control who can and cannot see your profile and private posts.

Visit us at **telus.com/wise**

Social networks and mobile application tips

1. **Keep an eye on your permissions settings.**
   Every time you download a smartphone app or sign up for a social networking site, you could be allowing its developers to see your personal information which could include your address book, your Facebook or Twitter account information, your location, or even your photos.

2. **Keep an eye on your privacy settings.**
   Make sure you know what information is being shared publicly — and what information can be accessed by applications. You may be sharing more than you intended.

3. **Think twice before connecting or posting.**
   It's a good rule of thumb to only connect and share with people that you know in real life. By 'friending' people online that are strangers, you open yourself up to added privacy and security risks. Facebook estimates that 7 percent of their users' profiles are fake, potentially created by malware writers and spammers. Also be careful with what you post and share. For example – posting pictures of yourself or others in inappropriate situations can hinder careers and dreams!

4. **Choose applications carefully.**
   Purchase/download applications from your smartphone or service provider's 'app store'. Stear clear of applications that ask for access to data like your address books, picture gallery, etc. Rule of thumb: Before downloading an application, do a search to make sure it's legitimate.

5. **Don't forget to log off.**
   Don't leave social media accounts (e.g. Twitter, Instagram) or applications/games (e.g. Angry Birds) open if you are not using them. If you don't log off you can become vulnerable to security and privacy risks. Also unsubscribe from accounts and apps that you aren't using. Think about this – a dormant Facebook account of a Calgary teen, who stopped using it because it had been previously hacked, was used to lure teens over the Internet by a criminal.

6. **Keep your digital household clean.**
   Set a time in your calendar every three to six months for you and your family to check your privacy and permission settings on the social media sites you subscribe to and apps you have downloaded. And don't forget to include your parents and grandparents – did you know that more than 40% of Canadians over the age of 65 are active on social media, primarily to keep in touch with their kids and grandkids!

4. General Internet tips

Courtesy of TELUS WISE

General Internet tips (for computer, laptops, tablets and smartphones)

1. **Set strong passwords.**
   A good password can help stop someone from hacking into your social networking accounts, email, smartphones or changing passwords on your applications. A good password is at least six characters (numbers, letters, etc.) long. You can make your password stronger by using the first letters of a phrase, instead of a word — ICARMLP for "I can always remember my laptop password", for instance — and changing some letters into numbers or other characters.

2. **Accept software upgrades from your smartphone, computer and software provider.**
   There are usually very important security patches that will protect your smartphone and/or computer from viruses.

   Generally, you want to use the features of the device or software manufacturer to get updates and you want to install the updates as soon as they are available to minimize your risk.

   For smartphones, the three major manufacturers will all offer their own programs to update the software on your phone. Blackberry, Apple and Android all have software managers that tell you if there is a new version of software available for your device or an application on your device. It is a good idea to only install applications and software updates from these authoritative sources. If you load software from a source that is NOT the manufacturer you have less ability to detect if the software is legitimate or safe.

   Similarly, on your computer, all your software updates should come from the manufacturer of the software. A great example of this is the large operating system vendors (like Microsoft and Apple) who manage large majority of the patches your devices will need and have been reliably doing this for years.

   You can usually trust updates that come from the manufacturer of the software that you are using. Adobe Systems, Skype, etc, are all examples of software that falls into this category.

   You should not install updates from sites that are not related to the manufacturer of the software. For example, don't install a Microsoft patch from "Bob's web site". This is likely less reliable than getting it directly from Microsoft.

3. Create a Google alert for your and your children's names to track how your name(s) are used online.

Just go to www.google.com/alerts and type in your name in quotation marks and enter your email address. You will receive Google alerts via email when your name appears online. This is not a 100% guarantee but a great start to tracking your digital footprint.

4. Keep your browser in check.

The web browser you use (e.g. Internet Explorer, Firefox, Google Chrome, Safari) is your gateway to the Internet and the first point of defence against malicious activity. Make sure you have the latest version of the browser installed and that it is configured to provide the desired levels of security and privacy. Also clear your browser history and cache at least one a month.

5. Be careful about sharing personal information and where/how you share it online.

In order to limit the amount of potentially sensitive information about yourself — and to limit your susceptibility to theft or abuse — think twice before posting:

- Your contact information (e.g. cell phone number)
- Your full date of birth
- The names of your children or family members
- Your full home address, where your children go to school
- Dates and details of trips, vacations and time spent away from home

When you are asked to share personal information online ask yourself the following questions: How it will be used? Why is it needed? Who will have access to it? And, how will my personal information be safeguarded? Remember it is YOUR information.

6. Think before you click.

Never click on suspicious links, even if they look interesting. A lot of scams and malware in the social network world are spread through links and rogue applications.

You should not respond to phone calls or emails that request personal or financial information, especially those that use pressure tactics or prey on fear. Legitimate service providers **will not** initiate communication with you and then ask you to provide or verify sensitive information through a non-secure means, such as email. If something seems suspicious or too good to be true, it most likely is, so pick up the phone and call your service provider or financial institution directly to verify the validity of an offer or request for account information. Finally, read your monthly account statements thoroughly as soon as they arrive to ensure all transactions shown are legitimate, and verify the transactions you expected to appear as well.

7. **When shopping or sharing sensitive information online ensure the url starts with https vs http or a picture of a lock in the browser.**

   Generally, try to use reputable sites. Anyone can ask you for your credit card, but it is less likely that a large, well-known company will put your credit card information at risk than a smaller one that doesn't have a track record of securing financial transactions. Check with friends or online references (not affiliated with the site) to get a feeling for reputability.

   Next, ensure that the site that you enter your credit card information into uses encryption. Look for the 's' in the http web link name, or look for the 'lock' symbol in your browser to indicate that encryption is being used.

   Additionally, there are features that each card provider offers that may help. Generally, credit card is safer than debit as it is insured against fraud. Similarly, some credit card companies offer a second, additional password that you can set up for Internet transactions to make it harder for criminals to steal and use your card number. There are also external services, such as Paypal, that have become trusted providers of credit card information and offer a way to protect your credit card information behind additional security.

5. General smartphone tips

Courtesy of TELUS WISE

Smartphones and tablet tips

1. **Turn off geo-tagging.**
   Turn off geo-tagging on your smartphone and tablet to enhance your privacy. When geo-tagging is turned on the exact latitude and longitude is included in photos you take and post on a social networking site or share or email. Geotagging can be found in your camera settings.

2. **Install or activate remote locate/lock/wipe software for your smartphone.**
   Some smartphones come with an optional service that will help you locate your phone if it's lost. Take advantage of this free service and set it up on your smartphone.

3. **When using public Wi-Fi networks at a minimum ensure the Wi-Fi network has security turned 'on'.**
   Be careful about using "free" Wi-Fi in public places – it can be an easy way for hackers to access personal information. Because it is broadcast over the airwaves and is not a service dedicated to you, it may be possible for others to monitor those same airwaves and see what you are doing. Stop and think about how secure the Wi-Fi might be before accessing it.

   Don't share personal or financial information over an unsecure network like public Wi-Fi unless you are confident it will be effectively encrypted.

   At a minimum, look for Wi-Fi networks that have security turned 'on', look for a lock symbol by the Wi-Fi account in your settings. In addition, try to only enter personal information (if required) into web sites that offer encrypted communications.

   Encryption ensures that the site you are sharing information with - the url beginning with https ("s" indicating secure) or sites that have a small lock icon in their address window are secured sites that encrypt your personal data so it can't be seen by anyone other than the intended recipient.

6. Protecting yourself from identify theft

Courtesy of the Royal Canadian Mounted Police

This section, courtesy of the RCMP, provides great information on how to protect yourself and your family from becoming a victim of identify theft. Further information can be found at **http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm**.

Identify theft

What is Identity Theft?

Identity theft refers to the preparatory stage of **acquiring** and **collecting** someone else's personal information for criminal purposes.

What is Identity Fraud?

Identity fraud is the actual deceptive **use** of the identity information of another person in connection with various frauds.

What is the Potential Impact on Victims?

- **Damage to credit history status**
- **Refusal of credit** (mortgages, loans)
- **Assumed identity** (offenders may incur criminal records or warrants)

What Information is Sought Out by the Fraudster?

- Full Name
- Date of Birth
- Social Insurance Number
- Full Address
- Mother's Maiden Name
- Username and Password for Online Services
- Driver's License Number
- Bank Account Numbers
- Personal Identification Numbers (PIN)
- Credit Card Information
- Signature
- Passport Number

How is Your Information Used?

- Access your bank accounts
- Open new bank accounts
- Transfer funds
- Apply for loans, credit cards and other goods and services
- Lease cars or apartments
- Hide criminal activities
- Obtain passports
- Receive government benefits

Some ways your personal information can be accessed are:

Physical theft – Fraudsters will:

- Steal purses and wallets
- Break into vehicles and homes

How to protect yourself

- Do not leave your purse or wallet out in plain view while at home, work, during recreation time or in an unattended vehicle
- Memorize your passwords and PIN's
- Do not carry important personal information documents with you unnecessarily

Theft of mail – Fraudsters will:

- Go to the same houses over and over again, to keep gathering information and build an information profile
- Intercept your mail in order to retrieve new cards

How to protect yourself

- Deposit outgoing mail in post office mailboxes or at your local post office
- Remove mail from your mailbox promptly after delivery
- Ensure you file a Change of Address Notification with Canada Post and advise all your financial institutions of your change of address before you move
- When unable to pick up your mail for any reason, have it collected or file a 'hold mail' request

Dumpster diving – Fraudsters will:

Go into dumpsters and sort through garbage looking for:

- Bank Statements
- Credit Card Invoices
- Utility Bills
- Pre-Approved Credit Cards

How to protect yourself

- Your trash is an identity thief's treasure! Be careful what you throw out. Your recycling bin and building garbage containers may be vulnerable. You have no "Expectation of Privacy" once your trash is on the curb.
- Shred anything and everything that holds personal information. This includes items with your signature, any account numbers, your social insurance number, medical information and legal information.
- Computers and cell phones contain a wealth of information that data thieves would love to get their hands on. Simply deleting your files and emptying the recycle bin is not enough; wipe or erase your hard drive before disposing.

Shoulder surfing– Fraudsters will:

- Look over a victims shoulder while they are entering in their PIN
- Listen in on someone's telephone conversation

How to protect yourself

- Make yourself more difficult to take advantage of
- Be aware of your surroundings and realize that shoulder surfers are actively seeking opportunities
- Avoid long lines or busy areas
- Block your data. Shield the number pad to prevent someone from stealing your PIN

Telemarketing scams - Fraudsters will:

- Trick the victim into divulging their personal information
- Pretend to be representing reputable agencies

How to protect yourself

- Before you provide your personal information, always ask for the reasons for the request to see if it is valid
- If you are unsure of the legitimacy of the call, contact the company and ask questions
- It is OK to hang up the phone when you are suspicious about the company calling

The Internet – Fraudsters will:

Find their victims on the Internet with minimum cost.Two common ways are:

- Phishing: the activity of defrauding an online account holder of personal and financial Information by posing as a legitimate company
- Pharming: the act of domain name switching, where you will be redirected from a legitimate website to a fraudulent site where your information is not secure and the fraudster can receive it

How to protect yourself

- Be particularly wary of unsolicited e-mails
- Choose passwords that will be difficult to crack
- Use different passwords for all accounts
- Change your passwords and PIN codes often
- Remember passwords without writing them down

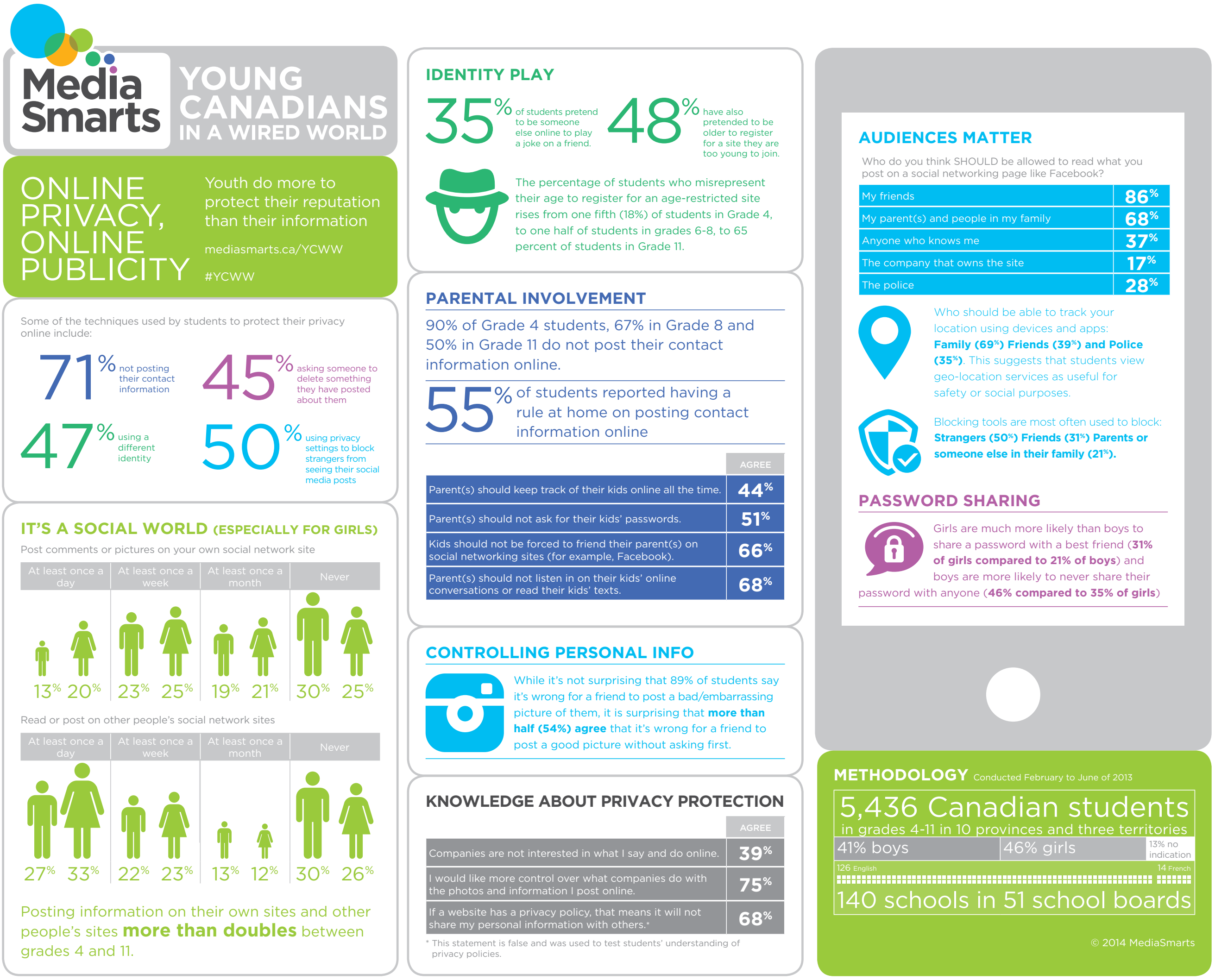
What to do if you are a victim

- **Step 1:** Contact your local police force and file a report
- **Step 2:** Contact your bank/financial institution and credit card company to make a report
- **Step 3:** Contact the two national credit bureaus and place a fraud alert on your credit reports
  - Equifax Canada Toll free: 1-800-465-7166
  - TransUnion Canada Toll free: 1-877-525-3823
- **Step 4:** Always report identity theft and fraud
  - Contact the Canadian Anti-Fraud Centre
    Toll free: 1-888-495-8501 www.antifraudcentre-centreantifraude.ca

7. Young Canadians' online privacy and online publicity

Courtesy of MediaSmarts

This report is drawn from a national survey of Canadian youth conducted by MediaSmarts in 2013. The classroom-based survey of 5,436 students in grades 4 through 11, in every province and territory, examined the role of networked technologies in young people's lives. Online Privacy, Online Publicity (the second in a series of reports from the survey) explores the Janus-faced nature of online privacy by examining the strategies that young people use to control how they are represented online and the ways in which they seek to assert some sort of control over their personal information.



MediaSmarts

YOUNG CANADIANS IN A WIRED WORLD

ONLINE PRIVACY, ONLINE PUBLICITY

Youth do more to protect their reputation than their information

mediasmarts.ca/YCWW

#YCWW

Some of the techniques used by students to protect their privacy online include:

71% not posting their contact information

45% asking someone to delete something they have posted about them

47% using a different identity

50% using privacy settings to block strangers from seeing their social media posts

IT'S A SOCIAL WORLD (ESPECIALLY FOR GIRLS)

Post comments or pictures on your own social network site

At least once a day		At least once a week		At least once a month		Never	
13%	20%	23%	25%	19%	21%	30%	25%

Read or post on other people's social network sites

At least once a day		At least once a week		At least once a month		Never	
27%	33%	22%	23%	13%	12%	30%	26%

Posting information on their own sites and other people's sites **more than doubles** between grades 4 and 11.

IDENTITY PLAY

35% of students pretend to be someone else online to play a joke on a friend.

48% have also pretended to be older to register for a site they are too young to join.

The percentage of students who misrepresent their age to register for an age-restricted site rises from one fifth (18%) of students in Grade 4, to one half of students in grades 6-8, to 65 percent of students in Grade 11.

PARENTAL INVOLVEMENT

90% of Grade 4 students, 67% in Grade 8 and 50% in Grade 11 do not post their contact information online.

55% of students reported having a rule at home on posting contact information online

	AGREE
Parent(s) should keep track of their kids online all the time.	44%
Parent(s) should not ask for their kids' passwords.	51%
Kids should not be forced to friend their parent(s) on social networking sites (for example, Facebook).	66%
Parent(s) should not listen in on their kids' online conversations or read their kids' texts.	68%

CONTROLLING PERSONAL INFO

While it's not surprising that 89% of students say it's wrong for a friend to post a bad/embarrassing picture of them, it is surprising that **more than half (54%) agree** that it's wrong for a friend to post a good picture without asking first.

KNOWLEDGE ABOUT PRIVACY PROTECTION

	AGREE
Companies are not interested in what I say and do online.	39%
I would like more control over what companies do with the photos and information I post online.	75%
If a website has a privacy policy, that means it will not share my personal information with others.*	68%

* This statement is false and was used to test students' understanding of privacy policies.

AUDIENCES MATTER

Who do you think SHOULD be allowed to read what you post on a social networking page like Facebook?

My friends	86%
My parent(s) and people in my family	68%
Anyone who knows me	37%
The company that owns the site	17%
The police	28%

Who should be able to track your location using devices and apps: **Family (69%) Friends (39%) and Police (35%)**. This suggests that students view geo-location services as useful for safety or social purposes.

Blocking tools are most often used to block: **Strangers (50%) Friends (31%) Parents or someone else in their family (21%).**

PASSWORD SHARING

Girls are much more likely than boys to share a password with a best friend (**31% of girls compared to 21% of boys**) and boys are more likely to never share their password with anyone (**46% compared to 35% of girls**)

METHODOLOGY Conducted February to June of 2013

5,436 Canadian students in grades 4-11 in 10 provinces and three territories

41% boys | 46% girls | 13% no indication

126 English | 14 French

140 schools in 51 school boards

Executive Summary – Key Findings

Young Canadians' immersion in social networking activities, as highlighted in the MediaSmarts report Online, provides the context for understanding young people's attitudes and behaviours relating to privacy. While students are willing to post information about themselves and their personal lives, they have very clear ideas of who should – and should not – be able to see what they post. They've also developed a number of strategies to help them manage their online reputations, but their limited understanding of data privacy issues and tools shows the need for more effective privacy education.

It's a Social World

Older teens are particularly active users of social media and frequently post information about themselves online.

- Ninety-five percent of Grade 11 students have Facebook accounts and nearly half of girls in grades 7-11 have Instagram and Twitter accounts.
- Grade 11 students (at least once a day or once a week):
    - Post comments or pictures on their own social networking sites (50%)
    - Read or post on other people's sites (73%)
    - Tweet (44%)
    - Follow friends and family on Twitter (39%)

However, sharing personal information starts early. A significant percentage of younger students have social media accounts and many of the virtual playgrounds that are popular with younger students also include social media, blurring the lines between online play and sharing information.

- Thirty-two percent of students in grades 4-6 have a Facebook account and 16 percent have a Twitter account.
- Eighteen percent of students in Grade 4, 28 percent of students in Grade 5, and 37 percent of students in Grade 6 report posting information on their own social media sites at least once a week.

Even with the high interest in social media, the majority of students don't post contact information online such as their home address or email address.

- This ranges from 90 percent in Grade 4, to 67 percent in Grade 8, to 50 percent in Grade 11.
- Household rules may play a role: more than half of students report having a rule at home about posting contact information online, and students with house rules are less likely to do whatever the rule suggests they avoid.

Identity Play as a Privacy Strategy

Previous Young Canadians in a Wired World research has highlighted how online identity play is used by youth for a number of different reasons. This latest phase is no exception, with significant numbers of students pretending to be someone else to play jokes on friends (35%) and flirt (13%). A large percentage of students also pretend to be someone else to protect their privacy, surf anonymously and bypass age restrictions on websites.

- Almost half (47%) of students have said that they were someone else online to protect their privacy.
- Close to one third (31%) of students pretend to be someone else to post comments on news or social media sites.
- Forty-eight percent have pretended to be older to register for a site they are too young to join.
    - The percentage of students who misrepresent their age rises from one fifth of students in Grade 4 to 65 percent of students in Grade 11.

Control over Personal Content, Especially Photographs

We know that young people's online experiences are social. But socializing is not necessarily the same thing as sharing. Students are very proactive about curating their online persona and controlling content that they don't want certain audiences to see – and a number of social norms have emerged around expectations regarding what friends share, and don't share, about their friends online. When it comes to photos, students apply a number of social and technical strategies to keep images that they want kept private out of the public eye, including using privacy settings to block certain people, deleting content themselves or asking others to take material down.

- While it's not surprising that 89 percent of students say it's wrong for a friend to post a bad/embarrassing picture of them, it is surprising that more than half (54%) agree that it's wrong for a friend to post a good picture without asking first. For French speaking students in Quebec, nearly three quarters of students think this is wrong (72%).
- For content that they have posted themselves:
    - Older students are more likely to delete content about themselves (77% have done so in Grade 11, compared to 77% who have never done this in Grade 4).
    - Their main concern is that parents (44%), family (42%) or friends (37%) will see it.
    - Girls are more likely to delete things, suggesting they are more concerned than boys about their online image.
- For photos that have been posted by others:
    - Ninety-seven percent of students would take steps to remove a photo they don't want others to see.

- The two most common strategies for doing this are to ask the person who posted it to take it down (80%) and to untag the photo (49%).
- French language students in Quebec are more likely than English language students in the rest of Canada to go to parents (53% compared to 35%) or teachers or principals (27% compared to 14%) for help.
- Overall, younger students are more likely to turn to adults if they need help. Turning to parents is the primary response for students in grades 4–8.
- As students get older, they are generally more accepting of friends posting photos of them without asking permission (by Grade 11 just over one quarter of students expect their friends to ask them first).

Audiences Matter

The attention paid by students to who can see photos and comments about them online underlines the importance of audiences to young people. Generally, audiences fall into three groups, with varying levels of exposure granted to each one. These include people in each student's social circle, institutional actors, and strangers and marketers.

People in Students' Social Circles

- When asked who should be able to see their photos and content online, the majority of students included people in their social circle: friends (86%), family (68%), and boyfriends/girlfriends (59%).
- However, even though they are comfortable being seen by their social circle, many students – especially older students – actively monitor what information friends and family have access to online. For example, students are more likely to use privacy settings to block friends (31%) and family members (21%) than any group other than strangers (50%).
- A majority of students (59%) say they would share the password to their social networking account, email account or cell phone, primarily within their social circle.
  - Not surprisingly, younger students are more likely than older students to say they would share their password with their parents, from a high of 66 percent in Grade 5 to a low of 14 percent in Grade 11.
  - While boys and girls were equally likely to share their passwords with a girlfriend or boyfriend, girls were much more likely to share passwords with a best friend.
  - Boys were more likely than girls to report never sharing their password with anyone at all.
- Even though many students are comfortable giving parents access to their online lives, a large number, especially of older students, think that parents should not constantly keep track of them online, force them to "friend" them, ask for their passwords or listen in on their conversations.
- Generally, French language students in Quebec are much more comfortable with parental monitoring (72% agree that parents should keep track of their kids online all the time, compared to 44% of English language students in the rest of Canada).

Institutional Actors

- Fewer students say that institutional actors, including police, government, social media companies and teachers/principals, should be able to see what they post on social media.
- Overall, students were more open to monitoring by police than teachers/principals and government:
    - Close to a third of students (28%) think police should be able to see their social networking posts and 35 percent of students agree that police should be able to track their location using devices and apps.
    - One fifth of students agree that government should be able to see what they post and 17 percent agree that the company that owns the social media site should be able to do this.
    - The vast majority of students (92%) believe that teachers and principals should not be allowed to use a device or application to check on a student's location (Table 12).
    - Only a small number of students (4%) think that a company that owns a device or an app that provides locational information should be allowed to check and see where they are.

Strangers and Marketers

- Over 90 percent of students think that strangers should not have access to their social networking page.
    - Although openness to strangers increases across grades, students are more leery of adults they have not met before than they are of people their own age.
    - Students are more likely to use privacy settings to block strangers than any other group.
- Older students are more likely to use privacy settings to block strangers than younger students (60% of students in grades 9-11 versus 25% of students in Grade 4).
- Only five percent of students think that marketing companies that want to advertise to them should be able to read their social network posts.
- One percent of students think that marketers should be able to track where they are.

Learning about Online Privacy Protections

Although students are generally well informed about protecting content about them that is posted online, there is a need for more education when it comes to corporate uses of their personal information. What students know – compared to what they think they know – about protecting their data is fraught with contradictions.

- Sixty-five percent of students have never had a privacy policy or terms of use agreement explained to them. There is a need for education here, as:
  - Sixty-eight percent of students mistakenly believe that "if a website has a privacy policy that means it will not share my personal information with anyone".
- French language students in Quebec are less likely than English language students in the rest of Canada to report that policies or agreements have been explained to them.
- While a majority of students (66%) say they have been taught about how companies collect and use their personal information, 39 percent agree with the statement "Companies are not interested in what I say and do online".
  - Almost one third (28%) of students agree with this statement: "I like it when companies use information I post to decide what products to advertise to me". This runs counter to students' feelings about marketing companies and companies that own social media websites being able to read their posts.
- The encouraging news is that 82 percent of students have learned about privacy settings.
- While parents are the main source of information (41%), one quarter of students have learned from friends and only 15 percent have learned about this from teachers.

Link to full report in English: **http://mediasmarts.ca/ycww/online-privacy-online-publicity**

8. Protecting our children from online exploitation

Courtesy of the Canadian Centre for Child Protection

Here are some tips from the Canadian Centre for Child Protection on protecting your children's privacy online.

Privacy and protecting Children from online exploitation (children 8-12 years of age)

- **Discuss the difference between public and private information.**
  Assist your child with the creation of online profiles when s/he joins social networking or gaming sites. Teach them to fill in only what is necessary, leaving out identifying or revealing information.
- **Explain to your child that s/he should trust her/his instincts and block anyone who asks questions online that seem 'weird**' (i.e. questions about puberty, sex, etc.). Explain to your child why it is important to tell an adult if this happens as it is likely this individual is behaving inappropriately with other kids too.
- **Reinforce the idea that not everyone is who they say they are online.**
  People can pretend to be older or younger than they actually are or they can misuse information you share with them. Talk to your child about only adding people s/he knows offline as her/his friends/contacts on social networking sites and apps.
- **Explain to your child that pictures/videos should only be shared between family members and friends.**
  Explain that once they are on the Internet, or sent through mobile devices, it is easy to lose control over what happens to them. It is important to encourage your child to check with you before sending or posting any pictures/videos online or through a smartphone.

Privacy and protecting teens from online exploitation (13-17 years of age)

- **Discuss online activities and popular sites and apps used by your teen.** Regularly engage in conversation with your teen about the applications s/he is using to connect with other individuals. Risks exist anytime children open themselves up to communicating with others on the Internet.
- **Discuss the qualities of healthy vs. unhealthy relationships.** In an effort to reduce the risk of teens being sexually exploited, it is important to teach them the difference between healthy versus controlling relationships. When a child is sexually exploited there is typically a distortion of the relationship and a misuse of trust by the offender.
- **Discuss the importance of adults demonstrating healthy boundaries with teens.** Explain that adults should not seek friendship with teens or give them any type of sexual attention. This is inappropriate behaviour and at a minimum, shows poor judgement - making it unsafe to interact with that adult.
- **Discuss direct and indirect ways of getting out of uncomfortable situations.** It can be very difficult for youth to get out of a situation that becomes uncomfortable or potentially unsafe, especially if they have an existing relationship with the person of concern.
- **Discuss the importance of seeking help.** Identify situations when it would be important to tell you, or another safe adult, about an uncomfortable or potentially unsafe situation. Acknowledge that while this may be a difficult step to take, you are there to help her/him and that her/his safety is your number one priority.

For additional information please visit **https://www.protectchildren.ca/app**

How you can participate in TELUS WISE

- Visit us at **telus.com/wise**
- Contact us at **wise@telus.com**
- Join the conversation online with **@TELUS** on Twitter and using **#TELUSWISE**