DATA DEFENDERS

Guide for Parents

Media Smarts

CANADA'S CENTRE FOR DIGITAL AND MEDIA LITERACY

Contents

Introduction

Although many young people care about their online privacy, most don't know how much information is collected about them and what they can do to limit this.

Learning about data collection at a young age is especially important, given that apps and websites aimed at children collect more data about their users than those aimed at adults!

By age ten, most Canadian children are already buying online services with their personal information. We need to help them understand not only how the platforms they use make money from their data, but also the ways in which this affects how – and how much – they share.

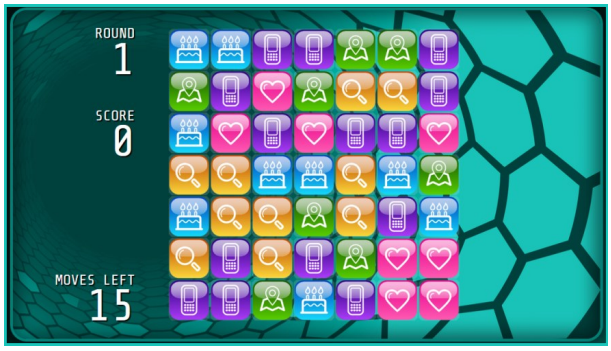
The *Data Defenders* game teaches children and pre-teens about personal information and its value, and introduces them to the different ways they can manage and protect their personal information on the websites and apps they enjoy.

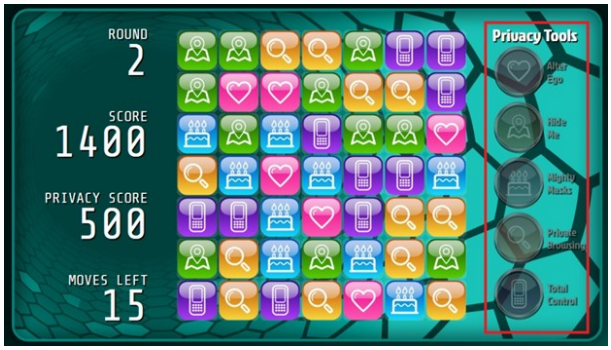
What is Personal Information?

Canada's *Personal Information Protection and Electronic Documents* Act defines personal information as "facts or subjective information about an identifiable individual." This can include your name, birthday, e-mail address and phone number, as well as your opinions, spending habits, IP address, photos and digital images, and e-mail and text messages.

Overview of the game

Data Defenders is a “match-three” game that introduces players to the idea that we pay for many online services and activities with our personal information. The game lasts two rounds.





In the first round, players try to get the highest possible score by matching tiles before they run out of moves. Each of these tiles represents five different types of personal information that companies typically collect: personally-identifiable information (such as your age, birthdate or gender), your browsing habits, your location, personal preferences (such as shows and videos you watch online), and information that’s on your phone (such as photos, contacts and apps you have downloaded).

At the end of Round 1, players discover that Algo Rhythm, the friendly computer who has been helping them to get extra turns, is actually an ad broker – someone who collects personal information to build user profiles, which are then sold to advertisers. Players also find out that in addition to their score in the match-three game, there’s also a hidden privacy score in the game that goes down every time you give information to the ad broker.

In the second round, players have a new goal in addition to matching tiles – to keep their privacy score as high as possible. To help them do this, they take quizzes that show them how to protect their privacy online and prevent them from losing privacy points.

Once they are completely out of moves, players get one of three ending screens, depending on how well they did. If needed, they are encouraged to replay the game to see if they can improve their scores (and get content and feedback they may have missed the first time around).

Suggestions for playing the game with your child

Data Defenders includes audio to assist children with different reading abilities. While the game can be played as a stand-alone activity, younger players will benefit from having a parent answer questions about some of the more difficult concepts and vocabulary in the quizzes and feedback. Here are some suggestions before you start:

- sit with your child while he or she goes through the game
- encourage your child to play through the game more than once to discover different feedback and to obtain a higher score (and a better ending!)
- play the game as well and compare and discuss the endings that you and your child arrive at

Note: Because the word “ad” appears throughout the *Data Defenders* game, some ad blockers may prevent it from playing. If you find that the game is not playing correctly, please add the *Data Defenders* web page (http://mediasmarts.ca/sites/mediasmarts/files/games/data-defenders/) to the list of exceptions (sometimes called ‘whitelist’) in your ad blocker settings and restart the game.

Reinforcing what you've learned

There are many ways that the privacy tools from *Data Defenders* can be applied in the real world. Here are a few tips that you can reinforce with your child after you've played.

Mighty Masks – Minimizing personal information

- The best way to avoid privacy risks is simply to limit how much personal information you give out. For example, when you're registering an account, only give out the information that's *necessary* (there's usually an indicator, like an asterisk or a different font colour, to show you what information is required and what's optional).
- When you're communicating with others online, avoid sharing personal information such as your age, where you go to school or your home address.
- Use a nickname instead of your real name; if that's not possible, make sure that your full legal name is not displayed (if your name is Michael, for instance, register as Mike).

Private Browsing – Privacy controls

- Browsers, applications and even games have privacy settings that let you control how much information you share. In some cases the settings will be part of the platform (a gaming console or a phone, for example) rather than the application itself. Privacy settings let you decide who can see if you're online, who can view your profile, who can chat with you, whether people can see your location and so on.
- Each platform has different types of privacy settings that may change from time to time, but you can always figure out where to find them by typing the name of the application or the platform in a search engine along with the keywords "privacy settings" (including the quotes). For example, if you are searching how to set up Chrome's privacy settings, typing in Chrome "privacy settings" will give you the link to official instructions on Google's website as your first search result.
- Finally, many browsers let you install "plugins" or "extensions" that are designed to block certain forms of tracking online. A good place to start is with Privacy Badger (https://www.eff.org/privacybadger).

Total Control – Controlling what your devices collect and what they share

- Our phones contain a LOT of our personal information: where we are at any moment, where we've been, who our friends are (from your contact list and from your social media apps), who we talk to the most, who we texted this morning, what we and our friends look like (from our photos), and much more! Until you take total control, a lot of people can have access to all that data. But you can put a stop to that!
- Get familiar with your phone's privacy and security settings. You can turn off many options on your phone that either collect or share your data. It can take some digging, but a web search with similar keywords to the search above (e.g. iPhone "privacy settings") will lead you to some instructions.
- Some of these privacy and security settings can get a little complicated (like app permissions), so another good trick is to look for online videos that show you how to set these.

Hide Me – Stopping your phone from signaling where you are

- Your phone needs to know where it is so that it can make and receive calls and help some apps work better (like maps, or tagging your photos with a location). You may have heard of GPS (global positioning system), which most smartphones use, but there are other ways that your phone can figure out where you are as well, such as through Wi-Fi and Bluetooth settings.
- Many apps on your phone can figure out where you are when GPS is turned on, and they sometimes broadcast that information to everyone else who is using the same apps! There are lots of reasons why you might not want broadcast your location and you can control this if you learn how.

Alter Ego – Recognizing sneaky data collection

- Apps and advertisers like to know what YOU like. It helps them show you ads, improve their services, and sometimes make money by selling your data. They can do this in many ways: by looking at what ads you click on; by asking you in sneaky ways like quizzes, surveys or contests; and by the videos you watch.
- One way you can help your child to recognize all of the sneaky ways that companies might try to collect personal data about them is to visit their favourite websites together and see if you can spot the different data collection techniques that are being used.

Additional resources

MediaSmarts resources

Digital Citizenship Guide for Parents

The *Digital Citizenship Guide for Parents* – which includes a section on kids and privacy – prepares parents and guardians for the conversations they should have with their children when they first start using digital devices.
http://mediasmarts.ca/parents/digital-citizenship-guide-parents

Helping our kids use their smartphones safely

This guide for parents helps them understand the issues around smartphones before deciding if their child is old enough to have one, including security and privacy.
http://mediasmarts.ca/parents/helping-our-kids-use-their-smartphones-safely-%E2%80%93-parent-guide

Related resources: Office of the Privacy Commission of Canada

What kind of information is being collected about me when I'm online?

The Office of the Privacy Commissioner of Canada has produced this fact sheet to help kids understand how their personal data is being collected online.
https://www.priv.gc.ca/youth-jeunes/fs-fi/choice-choix_e.asp

The Office of the Privacy Commissioner of Canada has also produced resources, tips and tools for teachers and parents to help them protect children's privacy and to discuss privacy issues with them.
https://www.priv.gc.ca/en/privacy-topics/privacy-and-kids/