The 4 Things You Must Do To Protect Your Data

Author : Cat

Date : June 18, 2014

It has been over a year since Edward Snowden outed the NSA for secretly spying on people using their digital data. This was a real eye-opener to the public, who once assumed much of their online information was safe. When we consider how much we do online these days (banking, bills, shopping, social networks), it is scary to think any of it may be vulnerable.

Who are we protecting our data from?

Government

Why does the government want your phone calls and your emails? They say it is to stop crimes, but we should question how much data they need to do that. Until very recently, government groups in the US and Canada could request your data from telecom providers *without* a warrant and without your knowledge. There are several group fighting this. OpenMedia.ca is one of several sites who are dedicated to teaching people about what information about you government can access.

Hackers

We are starting to see enough large scale violations of data privacy that it seems commonplace.

Here are four of the biggest and the kinds of information that was stolen:

- ***Heartbleed***: Spring 2014 bug in security software. Affected most major services, including email and online retail, where hackers could read data submitted via those websites (ex passwords, login, financial information).
- ***Adobe***: System was hacked and over 38 million login-password combinations were stolen.
- ***Target***: Christmas 2013, 40 million people had their credit card information stolen from the store's checkout.
- **eBay:** Encrypted user database was extracted from secure servers, including passwords.

Advertisers

Diaper advertisers only want to show their ads to parents of young kids. Conversely, parents of young kids are usually the only ones to buy diapers. Third-party advertisers want to know more about you so they can target their ads to the right people and so you see fewer ads you are not interested in. Depending on how you look at this, it could be win-win. The sketchy part is how they are obtaining that data and are you aware they are taking it.

How do you protect yourself?

1. Set different passwords for every account

I know, easier said than done. You have loads of accounts and how do you possibly remember all of your passwords? Consider this: if one account gets hacked (ex Facebook), then the hackers are able to run scripts against every other major service so they could get access to something else (e.g. your bank account) if it has the same login-password combination.

2. Check your privacy settings

Every network that allows you to post also has a set of privacy settings. Make sure you are aware where posts are public and where they are shared with a smaller audience. A good analogy is thinking about telling a secret to someone. Once you have voiced it, you are at the mercy of the person you shared with to keep that secret. That said, you have not told the world. Everything online is always permanent but you can select a trusted audience.

3. Only use secure sites

Whenever entering in your credit card information or any other personal identifiers (even your address) look for the 'https' or lock symbol in the address bar. This implies that your data is encrypted and can only be unlocked by the recipient of the data. If you are worried about cloud data being stolen, you can download an encrypting software to your laptop and secure the data before loading it to the cloud. This way, only you can decipher the data.

4. Beware phishing and malware

Phishing is the term used when you are asked for data under the pretence of something else. An example of phishing is an email that appears to come from your bank or cable provider asking you to sign in to your account via a link in the email. Real institutions and services should never ask you for your login via email nor should they be asking you to use their link.

Malware (or spyware) is software that is downloaded to your computer that takes or destroys information. The best way to avoid it is not to download anything from an email or website that is not trusted. Antivirus programs often protect against malware and spyware, and there are free utilities available for download to scan and clean computers.

Technology puts us at a crossroads between convenience and security. We want to use electronic services but there will always be some level of risk. At the very least, take the above 4 steps to protect yourself. And remember: Data can be protected, but nothing online should be considered completely private.