Personal Information Security Breaches

A compilation by Arlene Nora Arlow, President
updated July 16, 2019
www.addventive.com

Your server broadcasts your physical location while you are on the internet. Cloud-based software and online software require your personal information. You do not ever know what country the server is located in that stores your information.

With "Microsoft Accounts", you are "live" on the cloud, even if you don't want to be. Google Chrome monitors you on the internet and your Gmail emails are visible to the employees at Google.

There are ways to protect yourself: check your credit record at least every 2 years (TransUnion and Equifax); don't use wireless apps to do banking; don't use your "real" birthday in your online profiles; use robust antivirus software; delete temporary internet files and cookies weekly; use complex online passwords; change your passwords regularely; and turn your computer or tablet off when not in use.

Hackers are - on average - inside a server or network for 197 days before they are discovered - if they are discovered at all.

Here's a summary recognizable platforms, dates and number of people affected in recent memory (up to July 2019):

Platform	***Dates***	***# of people affected***
Yahoo	2013-2014	3 billion user accounts
Facebook	April 2019	540 million user records
Marriott International	2014-2018	500 million customers
Friend Finder	October 2016	412 million user accounts
eBay	May 2014	145 million users
Equifax	July 2017	143 million consumers
Target Stores	December 2013	110 million customers
MyHeritage Genealogy	October 2017	92 million customers
JP Morgan Chase	July 2014	76 million households & 7 million small businesses
Sony Playstation Network	April 2011	77 million user accounts
Uber	2016	57 million customers
Home Depot	September 2014	56 million customers
Adobe	October 2013	38 million user accounts
Bell Canada	2017 & 2018	2 million records
Desjardin Financial	2019	2.9 million
Walmart	2015	1.3 million customers

Source: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Source: https://en.wikipedia.org/wiki/List_of_data_breaches

DELL

In August, 2015, Dell began shipping computers with "eDellRoot", a Self-Signed root certificate that installs into the Microsoft Windows Trusted Root Certificate Store. Unfortunately, all "eDellRoot" certificates are installed with the same private key. This permits hackers to easily impersonate trusted websites; easily sign email messages; attach any publisher name to malware; and decrypt HTTPS traffic.

Source: https://securesense.ca/sayhello-edellroot/

LENOVO

In 2014, Lenovo began bundling snooping "Superfish" adware in its computers. "uperfish had a self-signed root certificate, potentially exposing the computer user's encrypted internet use. A hacker can spoof HTTPS sites and intercept HTTPS traffic without triggering browser certificate warnings.

Source: https://krebsonsecurity.com/tag/lenovo/

Source: http://www.smallbusinesscomputing.com/News/Security/lenovos-superfish-security-gaffe-trust-no-one.html

Source: http://www.eweek.com/security/lenovo-now-acknowledges-superfish-adware-risks.html

ADOBE

In August 2013 hackers gained access to one of Adobe's source code repositories, stealing credit card and password information of 2.9 million customers.

Source: https://krebsonsecurity.com/tag/source-code-leak/

Source: https://www.csoonline.com/article/3268035/adobe-s-cso-talks-security-the-2013-breach-and-how-he-sets-priorities.html

INTUIT - TURBOTAX

Intuit produces QuickBooks, Quicken, ProFile and other accounting softwares. TurboTax was the only platform that Intuit admitted was vulnerable to the Heartbleed Bug.

Source: http://www.sleeter.com/blog/2014/04/the-impact-of-the-heartbleed-bug/

FACEBOOK

July 13, 2019, FaceBook was fined $5-billion by the U.S. Federal Trade Commission following an investigation into privacy violations (investigations in Europe continued).

Source: https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/

Source: https://www.usatoday.com/story/money/2019/07/15/facebook-fined-5-billion-ftc-cambridge-analytica/39687137/

EQUIFAX

EquiFax Canada Inc. experienced security breaches in February 2004, June 2005, April 2015 and September 2017.

Source: http://www.itworldcanada.com/article/update-canadian-credit-agency-reports-security-breach/15395

Source: http://www.theglobeandmail.com/report-on-business/criminals-breach-equifax-again/article1120083/

Source: https://www.cbc.ca/news/technology/equifax-canada-breach-sin-cybersecurity-what-we-know-1.4297532

Source: http://www.databreaches.net/equifax-discloses-data-breach-due-to-technical-error-during-software-change/

Source: https://www.itworldcanada.com/article/after-suffering-huge-data-breach-equifax-tells-canadians-theyre-not-doing-enough-to-protect-their-data/415881

GLOBAL PAYMENTS

In April, 2012 the giant payment processing firm Global Payments announced a data center security breach that exposed 1.5 million credit and debit card numbers. The breach cost Global Payments $93.9 million. Global Payments admitted the breach lasted 18 months.

Source: http://krebsonsecurity.com/tag/global-payments-breach/

CANADA REVENUE AGENCY & THE GOVERNMENT OF CANADA

In November of 2014 CBC News announced Canada Revenue Agency had accidentally provided personal information to their news department.

Canada's privacy commissioner stated thousands of taxpayers' files had been inappropriately accessed by CRA employees for "personal gain, preferential treatment and fraud."

In August of 2014, Stephen Arthuro Solis-Reyes was charged with one count of unauthorized use of a computer and one count of mischief. He was able to get 900 SIN (Social Insurance Numbers) from a Canada Revenue Agency database. The 19 year-old Ontario university student used the so-called Heartbleed bug.

Canada Revenue Agency had to shut down its online tax filing system for several days in April of 2015 so that it could address security issues with the Heartbleed bug.

In March of 2014 the Government of Canada reported a spike in security breaches. In the 10 months ending January 2014, the federal government admitted to 3,763 security breaches. 2,983 - or close to 80% - of those known breaches were in the database of Canada Revenue Agency.

Source: http://www.cbc.ca/news/politics/stephen-solis-reyes-accused-in-cra-heartbleed-hack-has-case-put-over-1.2709556

Source: http://www.cbc.ca/news/business/taxes/tax-time-2015-how-safe-is-your-data-with-the-cra-1.2953519

https://www.itworldcanada.com/post/revenue-agency-bumps-up-government-data-breach-numbers

HRSDC-HUMAN RESOURCES AND SKILLS DEVELOPMENT CANADA

In January of 2013 HRSDC admitted that a portable hard drive containing the personal information of 583,000 Canadian students had been lost from an office in Gatineau, Quebec.

In November of 2012 HRSDC lost a USB storage device with personal information of 5,000 Canadians.

Source: https://lfpress.com/2012/12/28/personal-information-for-thousands-gone-missing/wcm/f33b5722-c1f7-feca-d0b0-7d5985ea1694

Source: https://torontosun.com/2013/01/15/feds-lose-student-loan-data-for-583000-people/wcm/294b9b56-be35-42f0-a9cf-81edca8d3548

SO YOU WANT TO LEARN MORE?

Paypal, Square and other payment methods have their own vulnerabilities:

https://www.zdnet.com/article/paypal-square-vulnerabilities-impact-mobile-point-of-sale-machines/

Here's a link for Canadian privacy breaches:

https://www.priv.gc.ca/en/opc-news/news-and-announcements/?q%5b0%5d=51&Page=1

The average security breach goes unnoticed for 197 days:

https://www.logichub.com/blog/data-breaches-are-taking-longer-detect-and-contain

Here's the top 5 reasons that data is breached:

https://www.whoa.com/data-breach-101-top-5-reasons-it-happens/

Everything you didn't know about data breaches:

https://www.wired.com/story/wired-guide-to-data-breaches/

++

About: Arlene Nora Arlow is an independent bookkeeper who specializes in using and tutoring for the QuickBooks desktop software. Her QuickBooks skillset is completely self-taught. She has been using QuickBooks since 1997. Arlene writes and sells QuickBooks learning guides from her website at www.addventive.com