How to protect your online privacy

Tommy Collison's simple but effective guide to online privacy and data protection.

In 2011, a prominent American venture capitalist, Marc Andreessen, wrote an op-ed in the *Wall Street Journal* about how so many industries —from agriculture to entertainment to national defense— were being changed by technology. “Software,” he declared, “is eating the world.”

And he’s right. The internet has enabled entirely new forms of communication and new types of businesses. It’s never been easier to start a new company, sell things online, and reach millions of potential customers.

But every action has an equal and opposite reaction, and the explosive popularity of the internet has also created new headaches for businesses. Hacking, identity theft, and other forms of cybercrime are rampant. Any business that stores personal information also has to be aware of the seemingly ever-changing regulation. In May 2018, the EU passed the GDPR, a sweeping privacy law that controls how user data is collected, stored, and used.

Are the hackers winning?

The last two years alone have shown that user data, in particular, is maddeningly difficult to keep secure.

Earlier this year, the personal information of millions of Facebook users was acquired by Cambridge Analytica, a data broker and consulting firm. The news that the organisation worked with pro-leave Brexit organisations rightly set many consumers on edge.

More worryingly, the US consumer credit reporting agency Equifax was hacked in 2017, exposing data on over 100 million users, including their full names and social security numbers (the American equivalent of our PPSNs).

At the same time, third-party trackers are growing in number. One study found that over 80 per cent of all websites—and a whopping 96 per cent of media and news websites—used cookies, making it easy for third-party tracking companies to build sophisticated files about unsuspecting individual internet users.

These files often include sensitive information about your location, income level, health conditions, or other things that could be gleaned from the websites you visit. One third-party tracker divides audiences into very specific segments, such as “burdened by debt: small-town singles,” so advertisers can better target them with ads.

The right thing to do

But it’s not just user data. As more and more of our information moves into the cloud, it’s crucial for businesses to have a firm understanding of network security and how to protect themselves from various online threats. Any business that has information on their users has to be deliberate about how they store that data and take steps to protect the privacy and security of their users.

Businesses generate other types of sensitive data, too: information on the organisation’s financials, for instance, or personal documents. Properly storing this data and encrypting it such that it can’t be accessed by unauthorised parties isn’t just good business practice — it’s also the right thing to do.

I work for the Tor Project, an American nonprofit that develops privacy and security software. The Tor network and browser are used by millions of people every day to communicate privately online and avoid being tracked and monitored as they browse the web. Everyday consumers, journalists, activists, health care workers, lawyers, government officials, and businesspeople rely on Tor to be safer on the internet.

Being secure online might seem like a Sisyphean task with the goalposts moving all the time, but it’s not as hard as you might think. Here are steps to help you and your business be safer online.

The simple steps to protect yourself and your data online

- Download Tor Browser, free software that protects you from being tracked, surveilled, or monitored as you browse the web. Tor protects users by concealing identifying information

with encryption as it travels over the Tor network, making unintended snooping and data collection virtually impossible. https://www.torproject.org/download.

- Encrypt hard-drives and servers containing users' personal information. https://advocacy.mozilla.org/en-US/encrypt-hard-drive.
- Use Onion Share to send and receive files of any size securely and anonymously. For sensitive documents, this is a much better choice than email or trusting a third-party like Dropbox or Google Drive. https://onionshare.org.
- Use two-factor authentication to secure your online accounts. This feature means that even if you're tricked into entering your password on a fake website, or if your password is posted online as part of a data breach, your account is still safe. https://twofactorauth.org.

Tommy Collison is an Irish writer living in Seattle, Washington. He works for the Tor Project (https://www.torproject.org/) and writes a technology column for the Irish Independent.