

We need to take responsibility for our own safety online

March 13 2015, by Shanton Chang



We need to take charge and teach ourselves a bit about the internet in order to stay safe online. Credit: gail/Flickr, CC BY-NC-ND

Going online without understanding the basics of how the internet works is like getting behind the wheel without knowing the road rules: you might still get where you're going, but you could be a danger to yourself and those around you.

Using the internet is now a daily activity for most Australians. Yet, the number of people who actually understand the internet's mechanics is small. Government and schools do work to promote [cyber security](#) and [cybersafety](#), but the message is still not getting widespread attention.

Ultimately there is only so much that government or businesses can do to keep us safe online. At a certain point, we need to take [personal responsibility](#) and educate ourselves about how to use the internet safely.

Rules of the road

A [recent book](#) on "cyberpsychology" and new media highlights the reasons why there has been a lag in awareness of cyber security. Much of it comes down to changing attitudes of [internet users](#).

Various studies have shown that there is a general lack of understanding about how the internet actually affects us. This is particularly the case since the advent of [Web 2.0](#), whereby we started posting user-generated content to the internet, some of it of a private nature.

Internet use has evolved quickly, and the rate of adoption of new applications has been phenomenal, outstripping the pace of regulation or research into internet use. When cars started hitting the roads in the early 20th century, they didn't change nearly as rapidly, and governments responded quickly through regulation and promoting new road rules.

While some of us are aware of the dangers of the internet, the idea that "it won't happen to me because I am not doing anything 'dodgy'" is a common fallacy. Car owners have insurance because they know that even if they drive carefully, they do not have full control of the environment and other drivers.

There is also a generally low level of digital literacy, including basic

things like knowing how a web browser works, what sources to trust and where uploaded information is stored.

This low level of digital literacy also contributes to the attitude of some parents and teachers, who proclaim it's impossible to keep up with their children. Therefore cyberspace is seen as the domain of so called "[digital natives](#)". Conversely, parents are able to instruct their children when they hop in the driver's seat.

Some people may also divest personal responsibility when it comes to cybersafety, preferring to trust government, via regulation, or business, through their own security policies, to protect them. Or they hope that their work or school will set up adequate firewalls.

This is problematic in that it is us who have final control in what we seek out, download, share or allow access to. Ultimately, firewalls are useless if the we freely provide the sensitive information to those who would misuse it.

Staying in our lane

In Australia there is a relatively strong culture of privacy and confidentiality. An example of this is shown by the [resistance to a national smart card](#) even just for health reasons, and the [national identity card](#).

This Australian interest in protecting privacy could to be harnessed to stimulate more widespread interest in [cyber security](#) more broadly.

However, it is important to understand the limits of Australian privacy laws and appreciate that it can be difficult to administer such laws. The internet does not have clear national boundaries making Australian laws potentially limited as most of us access sites internationally.

Christopher Kuner, a lawyer at Hunton & Williams, has written a [concise summary](#) of the progress of privacy laws internationally.

And just as a driver should know their vehicle and its limitations, we should know the basics of our browser settings and the privacy settings of any apps and software we might be using. In addition, as more are using the cloud, they should also be aware of the [conditions of using these services](#). After all, most drivers carefully pick the mechanic who services their car.

There is also a need for us to be aware of what we are sharing online. More importantly, with whom we are sharing it. It is easier than ever for strangers to get to know us just by looking at what we share through social media. Disparate pieces of information, even from different sites, can be pulled together to form a picture of us, making us an easier target for things like identity theft.

Getting behind the wheel

Finally, we should be aware of unfamiliar websites and the possibility of Trojans, malware and phishing scams.

Usually a simple Google search will yield a lot of information on how we can minimise these kinds of threats. Google itself also has pages of useful information on [online safety](#). We don't hand over our car keys to strangers, or let others know publicly where we keep them. Neither should we freely allow access to our personal devices or our private information.

Government regulation and business protections alone are not sufficient to keep us safe online. Just like on the roads, it also takes a measure of personal responsibility and a commitment to learn the basic skills required to use the [internet](#) to keep ourselves, and those around us,

protected from online threats.

This story is published courtesy of [The Conversation](#) (under Creative Commons-Attribution/No derivatives).

Source: The Conversation

Citation: We need to take responsibility for our own safety online (2015, March 13) retrieved 24 June 2024 from <https://phys.org/news/2015-03-responsibility-safety-online.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.