We must all take our cyber-security seriously

The tools for safe cyber-living exist. We need to feel they're relevant to us

The Observer, Sunday 3 February 2013

It has been a fragile week for cyber-security, with system breaches affecting a quarter-of-a-million Twitter accounts coming on the heels of online assaults against both the New York Times and the Wall Street Journal, apparently by highly sophisticated Chinese hackers.

Given the vulnerability of these high-profile targets, ordinary users might be forgiven for feeling any residual digital euphoria replaced by growing unease. What does it mean to be secure in an online realm where few people understand anything of the frantic combat taking place around them?

When it comes to combating online criminality, attempted cures can look as noxious as the disease. In Britain, the draft communications data dill – a "snoopers' charter" obliging mobile phone and internet service providers to record the details of all their users' actions – has proved sufficiently controversial for leading Conservatives to join Nick Clegg in calling for its overhaul.

Elsewhere, still more draconian legislation has been proposed in the name of preventing everything from piracy to political protest; earlier this year, the American programmer and activist Aaron Swartz became perhaps the world's first martyr to the cause of information freedom after taking his own life while awaiting trial – complete with the threat of punitive prison time – for downloading millions of academic articles.

As more and more of value in our lives migrates online, reconciling freedom of digital action with freedom from exploitation by others is only going to get trickier. A system is only as strong as its weakest component and many domestic users still leave the equivalent of at least one window wide open in their online abodes.

Most governments, experts and corporations would love us to close these windows. For all that burglary metaphors are apt, however, there remains a profound difference between fear of physical crime and the fear of digital disaster. And it's this emotional disengagement that is perhaps the biggest obstacle of all to individual safety online.

If you wanted to design a problem that people don't care about, behavioural economics professor Dan Ariely once argued, "you would probably come up with global warming", because its consequences are so distant in time and space from its causes. Similarly, most cyber-threat stories seem custom designed to disengage ordinary users. They're largely about other people or abstract possibilities, debated in obscure terms by experts who readily concede their inability to identify the next big threat.

There is also, however, a crucial difference between technology and climate change – because people do actually design digital systems, together with their vulnerabilities, defaults and enticements. We can't possibly anticipate every threat online and legislative attempts to do so are fated to fail. We can, however, try to change the terms in which we debate them and in which we share warnings, solutions and stories.

From encryption and good password "hygiene" to multiple-step verification, plenty of tools and techniques for safer cyber-living already exist. Nobody, however, bothers to close a window they don't know is open in a house they don't think of as their own. For all of us, that needs to change.