Hack of dating sites signals an end to promiscuous use of online identity

July 24 2015, by David Glance

Promiscuity. Credit: Flickr/Capes Treasures, CC BY-NC-ND

If anybody is still labouring under the mistaken belief that anything

online can remain private and secure, this week should have seen them finally admit defeat. In the US, UCLA Health reported) that 4.5 million health records had been compromised. UCLA Health runs four hospitals and 150 offices in Southern California, based at the University of California and Los Angeles.

The security breech joins a long list of recent hacks of health insurance, and health services, companies, including that of health insurance company Anthem that had up to 80 million customer records illegally accessed earlier this year.

More poignantly, and also this week, international dating site Ashley Madison admitted that hackers had accessed its systems and stolen details of its 37 million customers. The particular twist in this hack is that the site encouraged people in existing relationships to "cheat" on their partners and have casual affairs. Amongst information stolen by the hackers were details of customers' sexual fantasies, which the hackers threatened to publish if demands to close down the site completely were not met.

Companies that have been hacked normally follow up these events by announcing the increased security measures that they have taken, including hiring dedicated security staff. It is perhaps surprising that these companies didn't believe that they needed these measures before they were forced to by someone breaking in. This comes despite organisations like the EFF warning that online dating sites weren't implementing basic minimal security standards on their sites.

For the customers affected, however, companies implementing security measures after the fact will bring little comfort, as they face the serious consequences of having financial and personal information leak into the criminal and public spheres.

As a consequence of these and many other large scale hacks of public and private organisations, it is fair to assume that any information that is provided online can, and will, eventually end up in the hands of cybercriminals. This has to lead to a rethink of how we are handling identity on the internet and consequences for organisations that not only ask for inappropriate levels of detail about their customers, but also fail to implement stringent security measures to guard against the loss of unencrypted data that they do hold.

Consumers can, of course, take steps themselves to limit the amount of information they provide when sites ask for it. This can extend from saying "no" to sites wanting to store credit card information for future use, through to providing a fake name and address when asked for contact details.

For shopping online, the benefit of using services like PayPal, Apple Pay or Android Pay is that sites don't store any information about credit cards on their own systems. Using one of these services means that the site also doesn't have to know the customer's address, and certainly there would be no reason to provide their real address.

Parcels can be delivered to parcel delivery points offered by a range of companies, again not using a home address.

Even disposable phone numbers can be bought from companies like France's onoff app (there are equivalent services in most countries) so that a person's actual phone number doesn't have to be disclosed.

Likewise, disposable email addresses can also be used with sites.

The reality is, though, that most people will consider taking these steps too much effort and will just ignore the risks or live with them. Ultimately it will need the sites themselves to change how they do

business.

Alternatively, there would be a significant market for a new anonymising service to provide a way for customers to have a virtual profile that could be used on sites that only links back to a real identity for payment and delivery purposes. Of course, this would break a site's ability to track users and serve advertising to them and so there will be a ongoing conflict of interest where companies strive for real names, and customers increasingly battle against providing them.

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

Source: The Conversation