Is social media the weak link in the fight against cyber attacks?

January 20 2015, by Alastair Macgibbon

How secure is your social media presence? Credit: Flickr/Jason Howie , CC BY

Improved cybersecurity for governments and the private sector is expected to feature in US President Barack Obama's annual State of the Union Address delivered on Tuesday night (US time) to Congress.

The president is also keen to introduce measures to improve privacy and clamp down on identity theft online as part of his campaign to tackle

cybersecurity.

This comes on the back of a number of high-profile cyber attacks, including the recent so-called hacking of social media accounts linked to the US military's Central Command.

But Central Command wasn't hacked in the sense of having its internal computer network breached and confidential information exposed. Rather, its Twitter and Youtube accounts were momentarily hijacked by people supporting the terrorist organisation ISIS.

This highlights more of a vulnerability in the social media platforms we all seem to increasingly entrust our reputations to.

High-profile victims

Central Command is not alone in having is social media accounts compromised, just a very embarrassing victim. Both United Press International and the New York Post had their Twitter accounts hijacked last week with some potentially damaging information posted online.

They will not be the last either with so many high-profile social media accounts for governments, corporations, celebrities, identities, campaign groups and politicians, including the US president, making use of such third-party tools. All are potential prime targets for those who wish to hijack the accounts, whether it's just to cause mischief or to promote a more terrifying cause.

Let's not forget, these social media platforms have never really made any promises to us that they'll actively look after our accounts, let alone our data.

While the appeal of using online channels is clear – combined, Twitter

and YouTube alone provide access to an audience of more than 1.28 billion monthly users – these latest incidents show there can be a price to pay for outsourcing our reputation.

How could organisations who use these platforms have made this embarrassing (though not dangerous) situation less likely to happen?

Certainly there are ways to reduce the likelihood of compromise from an end-user perspective: hard-to-guess unique passwords that are changed often are the building block of internet safety and security, which I wrote about last year.

In addition, most of these sites offer versions of two-factor authentication, which involves things like sending verification codes via SMS to mobiles when changes are made to accounts. These practices alone will prevent most compromises, but are still relatively trivial barriers to determined hackers.

How secure is social media?

Really the problem is much deeper and stems from the dominant philosophy in large consumer-facing web companies – that accessibility and usability should only rarely be traded off for account security.

While there will always be a balance between utility and security, what is critical is for these companies to place value on the data and reputation of end users. They'll profess they do this, and in a macro sense they actually do. But it's a hard message for a loyal customer to swallow that their account slipped through the net.

The fact is, the convenience and massive consumer traction these sites offer come with a price.

If online services make it relatively easy to recover a password when a customer has forgotten it, criminals will exploit that. If you make it too hard, you risk legitimate customers giving up in frustration. The point of these platforms is all about maximising the number of people using them and the eyeballs that they bring.

I'm not beating up on organisations like Twitter. For a long time improved security would have indeed been at the expense of convenience.

But increasingly it is possible for these companies to deploy technologies that look for account compromises that don't impact on usability. Having a granular knowledge of the customer, such as their devices and their habits – which are so effectively exploited for marketing purposes on a daily basis – can be used to fight hackers and fraudsters.

When I was in the Trust and Safety area at eBay a decade ago those technologies were bespoke, expensive and temperamental. Now they are surprisingly cheap, robust and available off the shelf.

Reforms and responsibility

It's certainly welcome that the US president is taking cybersecurity so seriously. He appears to be taking a holistic approach where government can do more, companies providing services have obligations and end users are recognised as not just important to improving security but also as stakeholders who will benefit from that increased security.

Any reforms he flags in his State of the Union Address will help companies internally increase the value placed upon individual accounts and the end user information therein. This will in turn drive some of the more modern account security initiatives discussed above. A little bit of carrot and stick, and collaboration will do that.

When it comes to governments and other agencies using social media and other third-party tools, we must recognise that a large part of protecting against cyber attack also rests with the individual users and how they protect such accounts.

It's only when both – users and social media companies – improve their approach to online security that we will reach a situation where social media is no longer seen as the weakest link in any attempt to improve cybersecurity.

In the meantime, government agencies such as Central Command are caught between a rock and a hard place: the same people criticising them for their accounts being compromised would condemn them if they didn't use these services for communicating effectively with the public.

It's a tough world online.

Source: The Conversation