THE CONVERSATION
Academic rigor, journalistic flair

CyberJihad hacked US Central Command's Twitter – how secure is your own feed?

January 12, 2015 4.09pm EST

A screenshot from the account while under hostile control. Reuters

Author

Andrew Smith
Lecturer in Networking, The Open University

The Twittersphere is abuzz about the news on Monday that ISIS or their affiliates are suspected of hacking and compromising the US Central Command's official Twitter account. As of Monday afternoon in the US, the US Centcom's Twitter and YouTube accounts were shut down.

There will be considerable discussion about the impact, embarrassment and damage this has caused.

Whatever your opinion of the US government may be, the hack has raised the profile of a so called CyberJihad that has been developing over the last year.

Welcome to the CyberWar

You only have to stop and think back over the last year to see that cybercrime has been on the rise. Also, you don't need to dig deeply to see that ISIS – unlike many other similar organisations – have been busy developing their social media presence.

As criminals and terrorists become more adept, defence agencies worldwide are playing a continual cat and mouse game. Often there are attacks against national services, but these go unreported when the offences are successfully deflected.

So what about Twitter?

Twitter is not owned or run by any defence agency. It is a third-party organisation, entirely outside of the control of any governmental organisation. It is worth bearing this in mind. The attack wasn't directly against the US Central Command, but instead against their Twitter account.

Apart from the embarrassing publicity, this attack did expose a weakness. The hackers successfully shared potentially critical information, though some reports say what they posted was already publicly available. It will take informed analysts to authenticate the quality of the information shared, but everyone worldwide has seen this account being clearly hacked and the owners of US Centcom take their time in responding.

While under hacker control, @Centcom listed purported names and addresses of military personnel. Reuters

Is it easy to compromise your Twitter account?

The answer is both yes and no. Yes, there are many tools to compromise a Twitter account. I will not help you look for these as it is a criminal offence in many nations. But the answer is also no, it's not, so long as you take care to maintain your service.

I run more than one Twitter account. Recently, one was compromised briefly on Christmas Day. Fortunately, I have a rule that puts all my emails from Twitter into a folder on my phone. With the day's festivities in full swing, I could see that there was an 'unusual login' warning from Twitter which gave clear steps on what to do. I did not follow any link from the email, I went into Twitter via a trusted computer and changed my password, which is one I only use for this account, and deleted any unwanted posts. There are plenty of excellent guides on creating passwords.

It probably took me around five minutes to resolve; I am not the central command of a major world powers military. The potential embarrassment for you and me is considerably less newsworthy.

As a safeguard, most email applications allow you to create rules or flag priority senders. Having my

emails go to a folder means I can quickly see when any unusual activity occurs on my social media accounts. It gives me time to respond and hopefully recover the situation.

Meanwhile, US Centcom is getting considerable negative press over this attack. They reacted to the hack, but not quickly enough. As with national defence, governments need to remain vigilant and stay on top of social media accounts.

Cybersecurity **Twitter** **Jihad** **Cyber warfare** **ISIS**