

The Conversation

9 May 2012, 2.28pm AEST

Facebook welcomes hackers, if they wear a white hat



Jason But

Lecturer, Centre for Advanced Internet Architectures at Swinburne University of Technology

As reported late last week, Facebook is encouraging hackers to try hacking its security systems to find weaknesses.

Those who succeed will receive a reward of US\$500 or more and have their name added to a list of helpful hackers.

Given ongoing unrest about Facebook and its associated privacy issues, some may see Facebook's "White Hats" scheme as a cynical ploy to improve public relations.

But there are other, more practical, reasons.

Hacking to help

We often differentiate "black-hat" hackers (those seeking to do harm) from "white-hat" hackers (those probing systems to discover and repair unknown problems).

While white-hat hackers occasionally get bad press, the work they do is often important in keeping software and systems safe from those with more malicious goals.

The concept of employing third parties to attack a network, system or software is not new. Microsoft has a similar system for its software, while open-source software depends heavily on reports from users to identify and address potential problems.

The practice is so commonplace that companies, including BT, led by Chief Security Technology Officer, Bruce Schneier, offers a service whereby customers can contract them to have their systems monitored and "attacked" by experts.

Problems with white-hat programs can arise when hackers attempt to probe systems uninvited, as is often the case. It's easy to claim to be a white hat, even though one's actions might not necessarily be seen as such.

Fortunately, this grey area is often protected by legal provisions that can punish unauthorised "visitors" with criminal penalties.

Let me know

As is typical with white-hat programs, reported faults found by Facebook hackers will not be immediately publicised. This allows time for flaws to be confirmed and corrected before becoming public knowledge.



Could hacking Mark Zuckerberg's social media giant lead to a fruitful career? Hegemony77 doll clothes

Indeed, Facebook makes it clear that, to be eligible for a reward, hackers must “give us reasonable time to respond to your report before making any information public”.

And, as is often the case in white-hat programs, Facebook has added the proviso that attackers must behave ethically in not stealing private information, nor attempting to cause harm.

The novelty of Facebook’s approach is both the opening-up of the program to the general public and the offer of rewards.

The company’s executives doubtlessly realise that, with the amount of personal data being stored, they are a tempting target. Rewarding people who behave ethically might minimise that risk.

It remains to be seen how successful this strategy will be, particularly if some black-hat hackers get caught and then claim they were probing the system as per the current initiative.

But the move may inspire other companies to take a similar approach. In an article in the Guardian, British military cyber-security chief Major General Jonathan Shaw suggests the military might adopt a similar program.

What’s in it for me?

Other than the monetary reward, and fleeting recognition, why might Facebook’s initiative appeal to your friendly neighbourhood hacker?

Well, Facebook hasn’t said they’ll be hiring anyone from the White Hats program, but if they did, it wouldn’t be the first time they’ve employed a hacker.

In June 2011 Facebook hired George “GeoHot” Hotz, just two months after the 21-year-old was sued by Sony for hacking the Playstation 3 game console.

In 2009 Microsoft hired Johnny Lee, a modder who made a name for himself on YouTube by hacking the Wiimote controller for the Nintendo Wii game console.

In the same year, an Australian mobile app developer mogeneration hired Ashley Towns, a then-21-year-old who had made headlines after releasing the first virus to infect the iPhone.

At first glance, it doesn’t seem to make sense for such companies to advertise they hire people who once committed a crime. But if security is important to these companies – and we know it is – it makes sense to hire people with the best skills. And those people might well be hackers.

So far, the list of contributors to Facebook’s White Hat program stands at 115 but with the promise of financial reward, international recognition and even the smallest chance of being hired for one’s exploits, that list looks certain to grow.

Further reading:

The Role of White Hat Hackers in Information Security – Amit Anand Jagarine, Pace University

Copyright © 2010–2012, The Conversation Media Group