Facebook account theft is an epidemic in Vietnam. Youthful users, lack of awareness, and a culture of informal lending have created a perfect storm for hackers to abuse. Vietnamese youth require help to rapidly improve their awareness and use of cyber security best practices to stop the hacking craze.

How does a free iPhone sound to you? A contest to win a valuable prize is nothing unusual in Vietnam, a fast-growing consumer market where both domestic and foreign brands frequently offer giveaways.

When Quynh saw a Facebook post shared by a friend – about a draw to win an iPhone 6 – she thought nothing of clicking on the ad and entering the draw, which prompted her to log into Facebook again.

“About a day later, I received a text message to my phone that someone had logged into my Facebook,” Quynh says. “Right away I tried to log in, but my password had been changed.”

Quynh, who at 27 is a few years older and wiser than the average Vietnamese Facebooker, had let a lapse in security allow hackers to steal her Facebook account. But she at least had taken some steps to protect her personal profile: “I had set my account to allow me to reset my password via email and my phone number. I followed the guidance on Facebook and got a new password.”

Quynh was able to quickly reclaim her account with no damage or loss of information. But many of her friends were not so lucky, and either lost money or had to establish new Facebook accounts.
While social media account theft is a concern everywhere, in Vietnam it is an epidemic. Hacking is so common that some Facebook users simply assume it comes with the territory of being active on social networks. The limited information available indicates that both individual behaviour and wider cultural factors are at play. Facebook's security protocols are considered very strong – but there are some legacy accounts using ‘security questions’ that are particularly susceptible to attack.

**Facebook in Vietnam**

The number of active social media users in Vietnam has increased by 50 percent since January 2014. Facebook is by far the dominant social network, with 31.3 million accounts registered for a population of 90.5 million. Of these, 19.2 million are held by youth under 25 years of age.

But among the many requests for help and clarification on the Facebook corporate page, account theft stands out (it's called 'hacking' even if no code manipulation is involved). Over the past three years, 'hacking' keywords have appeared in 454 comments on Facebook's Page. Almost half of all 280 posts on the Page have at least one comment with a hacking query – normally asking Facebook for help to reacquire an account. These public requests for help likely represent only a small fraction of the total number of cases.

When *Tia Sang Vietnam* contacted 15 friends and former colleagues in Vietnam, one had lost their account, and six more knew at least one personal friend who had been hacked. One colleague saw two attempts to change her password in a span of two weeks in February 2015 (the hackers, from a Vietnam IP address, were not successful – she had recently set up two-step authentication to protect her account). Another case involved a Vietnamese community organizer in Ottawa, Canada. He had his Facebook profile stolen in 2014, including the community Page he managed, with all its contacts and information.

---


The raft of account theft, however, does not mean Vietnam is rife with highly skilled cyber criminals. As covered in a Tia Sang Vietnam blog post, most theft involves luck and guesswork, not advanced coding skills.

Long, an executive at an advertising company, had an old Facebook account that he hadn’t used in several years. He had friended many people on this old account, including strangers, and he had set a very simple, short password that was easy for both him and his girlfriend to remember. Long used many third-party applications on this account as well.

As his use of social media changed, Long eventually set up a new Facebook profile with tighter security settings, including two-step authentication.

He all but forgot about the first account until a friend called him one day to say that his old Facebook profile had been hacked – which he knew because he was chatting online with the hacker! Long rushed over to his friend’s place and sat down at the computer. Posing as his friend, Long told the hacker “Yeah I hate that Long guy, let’s get him.” Long then sent the hacker a list of other friends connected to his account that he said were “rich and naïve, you can steal from them.” He further established trust with the hacker by saying he was impressed by his skills and wanted to learn more about hacking. Long suggested they meet in person, and the hacker agreed.

Long asked the hacker for his age, the answer was 21 years old. Long said he did not believe ‘someone so young could be so skilful’ to hack a Facebook account. To prove his age, the hacker sent a photo of his state-issued personal identity card, high school certificate, and student ID card (Tia Sang Vietnam saw this photo).

The tables were turned, rather easily. Long eventually tracked down the hacker’s home address, and his current school, among other personal details. As neither Long nor his friends lost any money as a result of the attack, the hacker was not reported to the police, and this information was never used.

This is not a typical example – most ‘hackers’ are more sophisticated than Long’s 21-year-old antagonist. But it shows that account theft is so rampant that almost anyone can do it. Long’s friends were all knowledgeable enough to ignore the naïve hacker’s personal messages. But in many cases, account theft results in the loss of real money.3

---

3 In one case, a woman lost USD 2,000 to a hacker she thought was a personal friend. See: http://www.xaluan.com/modules.php?name=News&file=article&id=963140#ixzz3Yc6F93w
Technical inexperience and cultural factors

Facebook's ever-expanding user base in Vietnam is mainly youth under 25, who at risk due to a widespread lack of cyber awareness. The scan of Facebook's corporate Page for Vietnam showed many teenagers publicly posting their emails and even phone numbers in their requests for help. The lack of basic online security savvy is evident in their posts.

And yet there is no evident source of help for Vietnam's youthful Facebook users. Neither parents nor the education system were prepared for the social media revolution.

While 95% of Vietnamese between the ages of 15-24 are online, many of their parents are not. Even those parents who use the internet are unlikely to understand the risks posed by social media or how to deal with them.

The school system is also unprepared. While computer literacy investments are being made (by the Gates Foundation, among others), online safety is not a major focus of educational programming. The main safety concern in Vietnam is state- and corporate-level cyber security, given the rampant hacking attempts on servers in Vietnam. One leading report found that Vietnam had more cyber attacks from "state sponsored and nationalist adversaries" than any country in the world in 2014 - much of it linked to espionage related to Southeast Asia's maritime disputes with China.4

The near-constant low-level cyber war means all the attention is on protecting Vietnam's networks. Scant attention is paid to helping individual users with their foibles. Furthermore, like many governments, Vietnam has conflicting interests in promoting digital safety among its citizens - as this deters the ability to conduct domestic surveillance.5

Culture plays a role as well. Informal credit is as much a part of Vietnam's economy as street hawkers and wet markets.6 While 'formal sector' ecommerce is in its early stages in Vietnam, there is a culture of lending and remittances among friends and family that makes use of pre-paid codes for SIM cards as an easy way to transfer funds.

As new mobile and online payment systems have emerged, the culture of lending money has gone digital. Some 89 percent of mobile accounts are pre-paid, and one popular form of lending money is to provide top-up codes via text message or email. This form of lending may have emerged given the popularity of mobile games, many of which require in-game purchases that use the pre-paid value on SIM cards.

The codes can be entered into any phone on the appropriate network, and are almost as liquid as cash – a secondary market in top-up cards and codes has existed for many years. As the codes don't need to be entered into a phone to be resold, they are virtually untraceable and are a very convenient means for overseas transfers. As both media and anecdotal reports indicate, the hackers often spam friends' lists or make targeted requests for money to be sent via mobile top-up codes.

Overseas Vietnamese are also targeted. Hackers may even by searching out user accounts that are based abroad or have family overseas, identifying targets by personal account details or posts. Remittances are part of daily life for many Vietnamese families – when an uncle or cousin from overseas emails or texts to ask for a small amount of

5 Cyber education at the level of individual users in Vietnam focuses on software piracy and its link to security breaches. Beyond pirated operating systems, however, Vietnamese computer users are also notorious for using out-dated software. In 2014, Kaspersky Lab found that Vietnam had the world's top rate of Windows XP use. Windows XP is no longer supporting by Microsoft – meaning no more security updates. Even improved safety practices by users will not help if they are using devices susceptible to exploitation. See: http://www.kaspersky.com/about/news/virus/2014/16-37-per-cent-users-still-run-Windows-XP-Kaspersky-Lab-Statistics-Say
money, the victim might send it without bothering to phone directly and ask why it is needed.

Finally, there is the social media platform itself – and the ease of hacking young users who accept random, unknown 'friends,' do not understand phishing techniques, and do not take active steps to secure their accounts. Just as there are numerous ways to crack an egg, hackers are spoiled by a choice of methods.

Many older accounts have a ‘security question’ as a means of password retrieval. Even if the victim’s email address is not known, hackers can potentially access the account by answering the security question. If they’ve studied the victim’s profile and posts, the answer may be obvious.

A more sophisticated method is to infect a victim’s computer or smartphone with malware that includes keylogging software that captures all keystrokes, including email addresses, user names and passwords. Malware can be sent via infected .doc or .pdf files that specifically target a victim (for example, they mention details related to the victim’s professional work).7

Another common method is phishing – creating fake ads or log-in pages that request a victim's account details. As websites can be cloned very easily, producing a fake page or website is not difficult. A variation on this method is to fake the account of a real person. Hackers steal images and posts from one account, then request that person’s friends to 'accept friend' on the fake account.

In Vietnam, phishing and password reset requests seem to be the most common hacking methods. The hackers are aided and abetted by the mass of internet users who have little knowledge of how to protect themselves online. What is needed is more education, and the promotion of simple steps people can take to protect their accounts.8

Online guidance on how to protect against hacking is readily available in Vietnamese.9 What is lacking are outreach and education campaigns that engage youth on the dangers of social media use and the need for personal responsibility in the fight against account theft and hacking. Given Vietnam’s broader struggle with network attacks, there is a national imperative to strengthen cyber security. The starting point should be with youth awareness and skills in online safety.

---

7 This method is often employed by state actors against bloggers and activists.
8 Two-step authentication is the best single means to protect accounts from remote hacking using the most common methods outlined above. Without access to a victim’s mobile phone, hackers cannot access the account. While not foolproof, widespread use of two-step authentication would limit the options hackers face, perhaps even putting them out of business. VPNs are also excellent protection tools. Many VPN tools are available, but the choice between free versus paid versions might confuse some users or hinder adoption. Also, VPN use in Vietnam is associated with breaking firewalls to access blocked websites. As a result, official media sources do not promote VPN use as a security tool. That VPNs greatly help to protect users on public WiFi networks may not be well known.
9 See for example [www.nofirewall.net](http://www.nofirewall.net) or [www.lamsaodevao.com](http://www.lamsaodevao.com).