**Publication: Channel News Asia Online**
**Date: 23 November 2017**
**Headline: This is how your phone's e-wallet can be hacked**

## This is how your phone's e-wallet can be hacked

As digital payments grow in popularity, which is more secure – cash or cashless transactions? Talking Point investigates.

SINGAPORE: Some might expect a computer-savvy millennial like Mr Winston Ho, 23, to be an early adopter of electronic payment services on his smartphone.

But the president of the Singapore Management University's Whitehat Society, a group of ethical hackers, is paranoid about downloading e-wallet apps or any app linked to credit card or bank accounts. He prefers to stick to cash transactions mostly.

His concern, which he and fellow committee member Wan Ding Yao shared with current affairs programme Talking Point, is that untrusted apps and phishing SMSes are giving hackers easier access to phones as e-payments grow in popularity. (Watch the episode here.)

Said Mr Wan:

We were experimenting with some of the e-wallet apps from some of our local banks, and we found out that some of the security measures put in place were not foolproof.

While many people believe that passwords, two-step verification and fingerprint recognition on some e-wallet apps may be enough to stop cybercriminals, the duo are not convinced.

**BEWARE FREE CREDITS, MONEY**

The problem is that a hacker can fool a user into downloading a modified or disguised version of the e-wallet app – by promising free credits and money – which could be hiding hard-to-detect computer viruses like a Trojan, said Mr Wan.

"Who doesn't want free money, right?" he added. "If you choose to install the programme and grant it all the permissions that you wouldn't normally grant it, you're letting a hacker gain access to your phone."

The hacker could then retrieve data stored on the phone. And with such computer viruses, security measures such as passwords and thumbprints may be of little use, as hackers would still be able to intercept one's SMSs, cautioned Mr Wan.

If you receive a one-time password, (the hacker) would be able to go into your phone - maybe at night when you're sleeping so as not to raise any suspicions - and retrieve the OTP to authenticate (himself).

**Publication: Channel News Asia Online**
**Date: 23 November 2017**
**Headline: This is how your phone's e-wallet can be hacked**

Installing an app from an untrusted source would usually prompt a warning to pop up on one's phone – a warning one should heed, he advised, to reduce the risk of such attacks.
***(Read: Your phone number is all a hacker needs to track you, steal your info)***

**CASHLESS VERSUS CASH**

Mobile-payments company Liquid Group, however, argues that e-wallets are more secure than credit cards or cash, as they are equipped with features such as a password or a personal identification number.

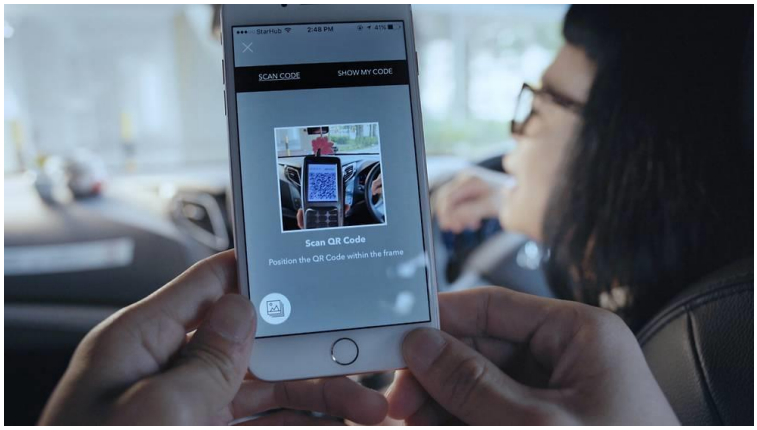
The company's chief executive officer Jeremy Tan said: "When you lose your card or cash, it's essentially gone. Whereas your phone, the first order or the first assumption is that the app in your phone has a certain degree of security."

He highlighted that consumers can track their transactions, and in the event of a fraud, the mobile payment company can trace the hacking.

Every single transfer is… trackable. So we tend to feel it's very silly if (someone) tries to hack into a digital wallet and move things around or pay (money into) different accounts.

"For us to find you is, I'd say, instant," he said.

DBS Bank, which launched e-wallet PayLah! in 2014 and allowed mobile QR code transactions this year, said that to protect its customers' money, it has introduced biometric verification, the first in Singapore with a Touch ID login that uses a fingerprint to access the e-wallet.



DBS Bank, which launched e-wallet PayLah! in 2014, has introduced biometric verification. (Photo: DBS)

DBS head of cards and unsecured loans Anthony Seow also explained that customers can set a limit to how much money they want their e-wallet to hold.

"Let's say you set it at $100. Then technically, (if) anybody has sent you, say, $300, only $100 would stay in there. The other $200 would go into your bank account," he said.

'FIRE DRILLS' ON YOUR PHONE

Singapore has a mobile phone penetration rate of 150 per cent, the highest in Southeast Asia. But it seems that users are not doing enough to protect their phones from cyber threats.

According to a Cyber Security Agency of Singapore (CSA) survey, one in three Singaporeans do not have anti-virus software on their phones.

**Publication: Channel News Asia Online**
**Date: 23 November 2017**
**Headline: This is how your phone's e-wallet can be hacked**

Crammed with personal and financial information, phones today have become a treasure trove of passwords, personal notes as well as credit card and log-on details. And the security stakes are growing.


File photo of a youth in Singapore using a mobile phone. (Photo: Francine Lim)

Cybercrimes here nearly doubled between 2014 and last year, rising from 7.9 to 13.7 per cent of all crimes, according to the inaugural Singapore Cyber Landscape report this year.

The CSA reported that 83 per cent of cybercrimes involved online cheating. Websites for banking and financial services were the most commonly spoofed, forming 31 per cent of phishing websites found last year. E-payment platform PayPal was also a popular target.

Mr Manjunath Bhat, a research director in Gartner's mobile and client computing group, noted that few people even know what is inside their phones.

He suggests that consumers conduct "fire drills" on their phones so that they know what to do if they lose their device. To prepare for such a situation, one only has to let a partner hold on to the "lost" phone.

"What you do is find out how much of the information that you have on your phone is now accessible to somebody else," he said.

"Think of it as: Can you cut off access to all the debit cards and credit cards as part of your digital wallet?"

He advises those who do lose their phone to put it in Lost Mode, which effectively disables the payment mechanisms. Alternatively, they could remotely reset the phone in this mode and wipe out the information inside.

DOES THE FACTORY RESET WORK?

But in a world of growing high-level fraud, does this delete all the data on the phone? And is a factory reset to purge a phone's memory sufficient, given how frequently people sell or trade their unwanted devices?

In an experiment for Talking Point, mobile forensic expert Ali Fazeli took some phones that had gone through a factory reset and managed to extract some information from them, including an SMS, some photos and older apps.

His company Infinity Forensics helps organisations and individuals recover deleted data and conduct tests against cyberattacks.

Yet despite his forensic skills, he could not retrieve any genuinely sensitive material on the used phones, which means that a reset phone may not leave a digital imprint after all.

**Publication: Channel News Asia Online**
**Date: 23 November 2017**
**Headline: This is how your phone's e-wallet can be hacked**

Still, for consumers, the key to keeping their phones safe is to be smart and vigilant as they move towards a cashless future.

Watch this episode of Talking Point here. New episodes air on Mediacorp Channel 5 every Thursday, 9.30pm.

Source: CNA/yv