Publication: Channel News Asia Online
Date: 09 January 2019
Headline: Why cybercriminals are stalking your social media accounts

Why cybercriminals are stalking your social media accounts

Are people giving away too much about themselves that it could come back to hurt them? The programme Why It Matters discovers how easy it is to extract personal information from social media posts and even name cards.

SINGAPORE: Just from his social media posts, it was easy to pin down radio deejay Joakim Gomez's running route, the street he lives at and even the layout of his home.

This came as a surprise to the 987FM radio personality, who had thought "it was harmless information I was sharing about myself". He declared: "I might just think twice before I post something at home."

Like many Singaporeans, Mr Gomez is active on social media. He posts live updates on what he's doing, tweets almost every day and shares pieces of his life with nearly 60,000 people who follow him on Instagram, Twitter and Facebook.

But he was revealing more than he realised.

Many people are similarly unaware of the extent to which someone with nefarious intent can extract all sorts of information about them from their social media posts, the free Wi-Fi they connect to or something as innocuous as their name card, as the programme Why It Matters discovers.

JUST A LITTLE SOCIAL MEDIA SLEUTHING

Three-quarters of people in Singapore actively use social media on mobile, according to Hootsuite's We Are Social report last year on global digital trends. By social media penetration, based on monthly active accounts, Singapore ranks third in the world.

In an increasingly cyber world, it is hard to avoid being online. But people often give away parts of themselves unwittingly by allowing people to view, download and share their thoughts, pictures and videos each time they post something.

With a little social media sleuthing, Why It Matters host Joshua Lim was privy to a ton of personal stuff about Mr Gomez – like date of birth, religion and even broadband subscription – before they met.

But it was the tracking down of Mr Gomez's housing precinct and being correct on where his room, the hall and the window were – from pictures he posted – that ruffled him somewhat.

"To actually get the layout of my house and … almost get my address correct – that one's a little scary," he said. "So this is a cause for concern."

Publication: Channel News Asia Online
Date: 09 January 2019
Headline: Why cybercriminals are stalking your social media accounts

It is potentially a security issue too, as he sometimes tells his listeners when he would be away from home and overseas.

He shares a lot online to connect with his listeners, but he has now begun to think about whether he is oversharing in terms of where he lives.

NOT JUST A NAME CARD

People often do not think about the information on their name cards either, but these contain personal details like the person's name, email address and, sometimes, personal mobile number – which can be the starting points for criminals.

To illustrate, armed with just Mr Lim's name and email address, cybersecurity company Horangi found his social media accounts, and pieced together his profile.

Horangi cyber operations consultant Cheng Lai Ki found out where Mr Lim lives, his family background, the model of his mobile phone and even where he went on his honeymoon. This is called open-source intelligence, publicly available information about someone.

Photos of one's honeymoon destination may be harmless, but what Mr Cheng warns against is to post pictures of one's mobile phone.

"Knowing the make and model of somebody's mobile phone, a hacker can essentially log into it by identifying the vulnerabilities it has," he said.

"Once they have access to your phone, they can read your emails (and) your text messages. They can access your contacts … your camera (and also) know the phone's location."

Given enough time, a hacker could find out where that person lives, from the pictures on his phone.

Mr Cheng advised individuals to be aware of what they post, especially with regard to photographs taken in the workplace, where there may be documents strewn on the desk or information on the computer screen.

N.R.I.C. MISUSE

There are other ways in which people could be making themselves vulnerable to criminals. One is through the National Registration Identity Card, which contains an individual's NRIC number, besides other data such as full name, photograph, thumbprint and home address.

The card can potentially unlock large amounts of information related to the individual, such as his medical records, insurance details and Central Provident Fund account information, according to the Personal Data Protection Commission.

This opens up the dangers of identity theft and fraud.

In the past 14 years, there were three incidents of NRIC misuse. For example, in 2005, a woman withdrew S$50,000 from her friend's bank account by showing her friend's NRIC to the staff, convincing them that she was the real deal.

But from Sept 1, organisations cannot collect, use and disclose NRIC data indiscriminately, and will not be allowed to make copies or retain the cards.

ROGUE WI-FI NETWORKS

Publication: Channel News Asia Online
Date: 09 January 2019
Headline: Why cybercriminals are stalking your social media accounts

Another way in which people can open themselves to an attack is through Wi-Fi.

A hacker can set up a rogue Wi-Fi network in public, and once you connect to it, the hacker can see every password you enter and every email you send.

He can also access your contacts and documents in what is called a “man in the middle” attack.

To get free Wi-Fi, people are sometimes asked to download an application first. But a hacker can use this app to access their location via GPS, record their conversations and access their camera and photos – all without them knowing.

According to cybersecurity firm Checkpoint Security, personal data is valuable and can be sold in online black markets. For example, an individual’s passport details and credit card information can sell for about US$30 (S$41).

PHISHING FOR INFORMATION

Finally, phishing is a form of fraud where an attacker pretends to be a reputable person or business entity to induce individuals to reveal their personal information, such as their passwords and credit card numbers.

In Singapore, victims lost at least S$43 million in email impersonations in 2017 - a 70 per cent spike from 2016. There were 328 cases of email impersonation in 2017, an almost 30 per cent jump from 257 cases in 2016.

Most of the victims were businesses who were deceived into transferring money to fraud bank accounts of their business partners.

Mr Wan Ding Yao, president of the White Hat Society from the Singapore Management University, advised individuals not to fill in any financial information when asked to do so because many reputable companies will not simply ask for financial details over a simple email.

“Whenever you are in doubt, always check, either through Google search, or just contacting the company if you are really unsure, and if the information asked of you is of great sensitivity,” he said.

In her book, “Fake it! Your Guide to Digital Self-Defense”, Danish author and journalist Pernille Tranberg suggests sharing our real identities only for official purposes - and switching to pseudo-identities when making accounts for sites and services that we don’t want mining our real data.

This means using a fake name, birth date, email, and even disguising ourselves to avoid facial recognition.

While this might conflict with the terms of service of social media sites like Facebook, which states that one should use their real name, the author advises readers to “disregard that”, as “your privacy is more important”.

Source: CNA/dp