SINGAPORE INSTITUTE OF TECHNOLOGY

Publication: The New Paper (Pg 2-3)
Date: 31 October 2016
Headline: Could this be your home?

Once a device is connected to the Internet, everybody can access it if you don't set up the fence properly.
— Associate Professor Steven Wong, the president of the Association of Information Security Professionals

VIEWING STREAM IS OK, UPLOADING IS NOT

It is not illegal to view the feeds that are on Insecam.

"Just viewing the feed does not constitute an infringement," said lawyer Gloria James-Civetta, managing partner of law firm Gloria James-Civetta & Co.

"It would be akin to watching an episode of a TV show that has been illegally uploaded on YouTube."

Mr George Hwang from George Hwang LL.C likens looking at the stream to someone looking through the open window of a Housing Board flat as they walk past on the corridor.

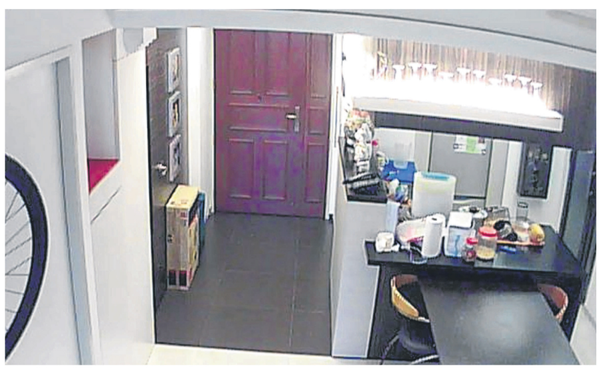
"There is no problem if you were just looking through that window," he said.

The infringement occurs if you put the stream online.

Said Ms James: "If a third party puts up a stream on the Internet, then that can constitute an infringement.

"There was no consent to taking someone else's data and letting the world see it."

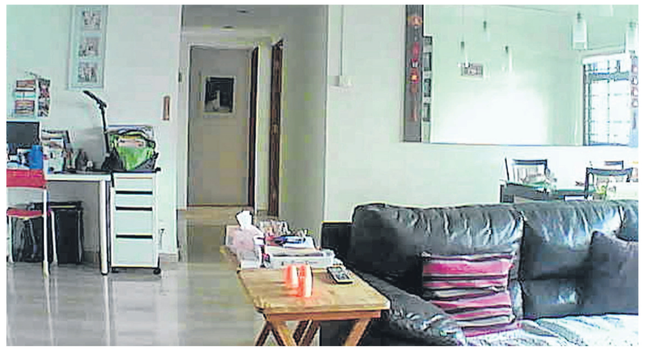
With just a few clicks, anybody can access the feed of your unprotected webcam



Manufacturers' advice? Change your default password

NEXTPAGE

Could this be your home?



Report by AZIM AZMAN
maazman@sph.com.sg

You could be unknowingly broadcasting your life on the Internet.

The website Insecam bills itself as a repository of unsecured surveillance cameras from all over the world, including Singapore.

With just a few clicks, anyone can access live images from places that look like the inside of offices, warehouses and homes.

The footage is from closed-circuit television and Internet protocol (IP) cameras. IP cameras work by connecting to a Wi-Fi network and their feeds can be viewed remotely from a smartphone or computer.

The New Paper first reported about it in 2014.

30 FEEDS

When monitoring the site last week, TNP saw more than 30 feeds from Singapore.

The website owners claim on the site that they constantly filter out cameras that intrude on the privacy of individuals.

However, some of the feeds clearly showed the inside of people's homes.

It gets worse.

Even if your webcam feed is not on Insecam, there are search engines that can scan for unsecured webcams, said Associate Professor Steven Wong, 41, the president of the Association of Information Security Professionals .

"In the digital world, it's just a fly through to collect (the addresses of these webcams)," he said. .

In a few short minutes, he showed TNP how easy it was for someone like him to tap into an unsecured webcam.

Using a search engine that was specifically built to find and map out devices connected to the Internet, he was able to look for the web addresses of webcams here.

A few taps of the keyboard was all it took for him to log on to unsecured webcams that were not listed on Insecam.

To prevent copycats, TNP is not naming that website.

How is this intrusion possible?

Such webcams are only protected by a default password or, worse, have no passwords at all.

"The most basic thing is the most dangerous thing," said Prof Wong, the programme director for the Information Security degree at the Singapore Institute of Technology.

He stressed that not changing the passwords to any device connected to the Internet leaves users vulnerable.

He said: "Once a device is connected to the Internet, everybody can access it if you don't set up the fence properly."

One user who wanted to be known only as Madam Ang, 45, said she was appalled by the content of Insecam.

She said: "The website claims to not intrude people's privacy, but I saw workplaces and I think somebody's home kitchen too."

When the admin assistant first bought her 7-Star security cameras more than three years ago, she had a family friend help her with them.

"My husband and I did not know how to use the camera back then so a friend came over to help set them up," she said.

Madam Ang has three cameras and they are used mainly to monitor the maid and to make sure the children come home on time.

She said there was no default password set-up for the cameras then and she was not aware of the risks of not setting a password.

She said: "Looking back, if our friend did not tell us to set a password, I would never have done it."

In an e-mail interview, Mr Nick Savvides, security advocate at security and technology giant Symantec said his company's analysis showed that web-connected or Internet of Things (IoT) devices are "scanned every two minutes".

"This means that a vulnerable device, such as one with a default password, could be compromised within minutes of going online," he said.

"Consumers should ensure that they are purchasing these devices from a trusted and reputable manufacturer."

The process of accessing unsecured cameras is easily automated.

Said Prof Wong: "Somebody can write a script that automatically scans through to find webcams which are not password protected."

Unsecured webcams also present a danger beyond having your privacy violated.

It can be used to launched a Distributed Denial of Service (DDoS) attack, similar to the one that affected StarHub users last week. (See report on the next page.)

BEING WATCHED: These are screenshots from the site that broadcasts feeds from webcams that have no password or just a default password.

PHOTOS: SCREEN SHOTS/INSECAM.ORG

TOOL

Mr Kelvin Lew, a cyber security consultant, said: "There are still millions of users who are not aware that their personal computers, devices and home equipment have become a tool for the hackers to do their illegal activities."

He urged IoT manufacturers to consider the security aspect in the design of their products.

So how can you prevent your webcams from being accessed?

Said Prof Wong: "Change your passwords!"

— Additional reporting by Elaine Lee