Publication: TODAY, p 1 & 8
Date: 7 June 2014
Headline: Online attacks a rising issue for companies, say IT experts

Online attacks a rising issue for companies, say IT experts

ALFRED CHUA
alfredchuamf@mediacorp.com.sg

SINGAPORE – As personal handheld devices become more powerful and capable of supporting applications that are more complex, they also become more susceptible to cyberattacks, warned IT experts.

And with more people using such devices to work remotely, these could make an organisation's system vulnerable to attack, they said, adding that, too often, organisations take little additional precautions until it is too late.

Their comments come in the wake of the revelation by the Infocomm Development Authority (IDA) on Wednesday that 1,560 SingPass user accounts could have been illegally accessed.

How this happened is still being investigated, but the IDA had stressed that there was no evidence at this point suggesting the SingPass system had been compromised.

It also said it would beef up security for the system, such as by possibly allowing users to set their own user names — instead of using NRIC numbers — and adding an additional layer of verification with two-factor authentication (2FA).

Mr Anthony Lim, a member of the Application Security Advisory Board at (ISC)2, a not-for-profit association for information security professionals, told TODAY that as smartphones become more sophisticated — with specifications not unlike those of personal computers — and applications on them get bigger, they become hotbeds for flaws and bugs, and hackers and malware can exploit these flaws.

As such, it becomes harder for smartphone and handheld device users to detect malware or viruses.

With the proliferation of such devices for work purposes, they "can form a gateway for viruses and malware to come into the organisation", said Mr Jan van Leersum, managing director of IT security firm Network Box.

Commenting on the cybersecurity practices of companies here, Mr Van Leersum said he has noticed that a lot of them tend to have simple firewalls. "They might think: 'Why

● CONTINUED ON PAGE 8

CYBERSECURITY TIPS

FOR PERSONAL USERS

- Regularly change passwords, and never use predictable passwords, such as birthdates
- Update anti-virus software regularly

FOR COMPANIES

- Use powerful network security platforms that can detect potential malware and/or virus attacks
- Have a 'no-work-data-leave-the-office practice' ensuring that if an employee loses a thumbdrive, mobile phone or laptop outside the office, there would be less fear of losing sensitive data

Online attacks a rising issue for companies, say IT experts

● CONTINUED FROM PAGE 1

should I take extra action if nothing is happening? Something simple would be enough'," he said.

Meanwhile, most organisations with computers accessible to the public or a large number of users that TODAY contacted said they take steps to ensure the safety of data in their computers, but they added that users must also be responsible for their personal cybersecurity.

A Changi Airport Group spokesperson said the cache on all the computer stations at Changi Airport is cleared when users log out, while the People's Association said it adheres to IDA guidelines on cybersecurity for the computers at its community clubs.

Similarly, a National Library Board spokesperson said: "The multimedia computers in our libraries are programmed to delete browser history and Internet cache upon logout."

A spokesperson from the Singapore Management University (SMU) said it has put in place "layers of defence" at its servers, but stressed that users have the responsibility to clear the cache in their computers and utilise the anti-virus software provided by SMU to protect their own computers and data.

IT experts agreed that these computers are most vulnerable — despite most being configured such that they do not store any user info — given the volume of usage.

Mr Lim added that the clearing of the cache was sufficient but cautioned against two potential issues.

The first, he said, was that most public computers "are not very well-maintained, which can lead to other problems that make them more susceptible to malware attacks".

Secondly, there is a risk of hackers installing malware on these computers that can track other users' personal data.

"Nothing can stop them from doing so," he said.

Mr Sharat Sinha, vice-president (Asia-Pacific) of Palo Alto Networks, said that, when using public computers that they have little control over, users should remember to clear all cache, cookies and history.

(ISC)2's Mr Lim added: "It is safest to stick to doing public things on public computers — like reading the news online, or checking maps out — and not do anything personal, such as making e-transactions." **ADDITIONAL REPORTING BY LOUISA TANG**