Yui Kee Computing Ltd.

Newsletter

April 2020

Contents

A Reminder of Old Advice

<web-link for this article>

Seventeen years ago, the South China Morning Post published a short article by Yui Kee Chief Consultant Allan Dyer. At that time, there was an increase in teleworking (now referred to as WFH, "Work From Home") due to the emergence of SARS. The article warned about increased information security risks due to this change in behaviour.

The information security landscape has changed many ways in 17 years, ransomeware has replaced computer viruses, but the advice is still relevant today: The home PC should be protected to the same level as the corporate network, install the latest security patches, and a VPN and endpoint security software are vital components in securing remote users. Businesses should educate home users about their vital role in strengthening corporate security.

Stay healthy. Stay secure.

Working from home opens door to other viruses

The foremost concern in Hong Kong has been the outbreak of atypical pneumonia, and many people are doing excellent work in fighting its spread.

Yet certain measures taken to prevent the illness from disrupting work or studies could lead to a different kind of outbreak: computer viruses.

What is the link between the prevention of atypical pneumonia and computer viruses? It is not in the recently discovered e-mail virus W32/Coronex.A, which exploits the health crisis by masquerading as a warning or an appeal for help.

Rather, the problem arises from the increased interest in teleworking, also known as telecommuting.

There are obvious security concerns when employees work from home, but that is what virtual private networking (VPN) is for. It creates an encrypted link between the office and the employee's home.

Combined with suitable access control, a VPN makes sure that only authorised staff are linked to the corporate network.

POINT OF VIEW
Allan Dyer

However, this set-up solves only one part of the security problem: the channel might be secure, but the end points are probably not.

It is hoped that the office already has adequate network security protection in place, but the average home computer is likely to be vulnerable.

Personal firewalls are not very common, and the only anti-virus software used might be the free version that was bundled with the PC when it was purchased.

This level of protection is hopelessly out of date. Under these circumstances, a hacker or virus can take over the home computer and access sensitive corporate information exposed via the VPN. Generally, viruses are indiscriminate. Since they can swiftly replicate, there is no limit to the number of simultaneous attacks they can make.

Many home PCs are probably harbouring a variety of viruses. Use of home PCs all day as part of a telecommuting set-up could give viruses more time to act. Staying online for a long stretch of time gives the viruses more time to spread. Connections to corporate intranets also give these viruses access to new address books to contact and new data to damage.

A large number of people teleworking, such as in Hong Kong at present, could create a situation in which computer virus incidents suddenly escalate.

One virus that could benefit from teleworking is the mass-mailing worm W32/Klez.H@mm. Known simply as Klez, it has been at the top of incident lists for most of the past year. Klez, like many viruses, e-mails itself to addresses it finds on the infected machine.

It also uses a different address in the "From:" field of the e-mail, so that the message appears to have originated from a different sender.

When it sends itself to new victims, Klez selects and attaches one of the user's files. This can easily result in confidential documents being sent to unauthorised people.

"Many home computers are probably harbouring a variety of viruses. Use of home computers all day as part of a telecommuting set-up could give viruses more time to act"

When an ordinary mass-mailing e-mail virus infects a machine, it sends out many messages. A PC user with up-to-date anti-virus software can easily detect this and send back a message warning the user of the infected machine that he or she is sending messages that contain viruses.

The user of the infected machine – who may not even care about viruses – is therefore pressured to do something about it. With Klez, however, this complaint or warning either gets sent to the wrong e-mail address or never gets sent at all.

So the user of the infected machine is never warned, which means that the infected computer may never get cleaned.

A computer virus that disrupts business can cause considerable economic damage.

The latest Labs Virus Prevalence Survey by the International Computer Security Association found that the median cost of a virus disaster to a company was US$9,500.

Three of the companies surveyed reported a cost of more than US$1 million for a single disaster.

Companies that implement teleworking must ensure the security of their remote-user systems.

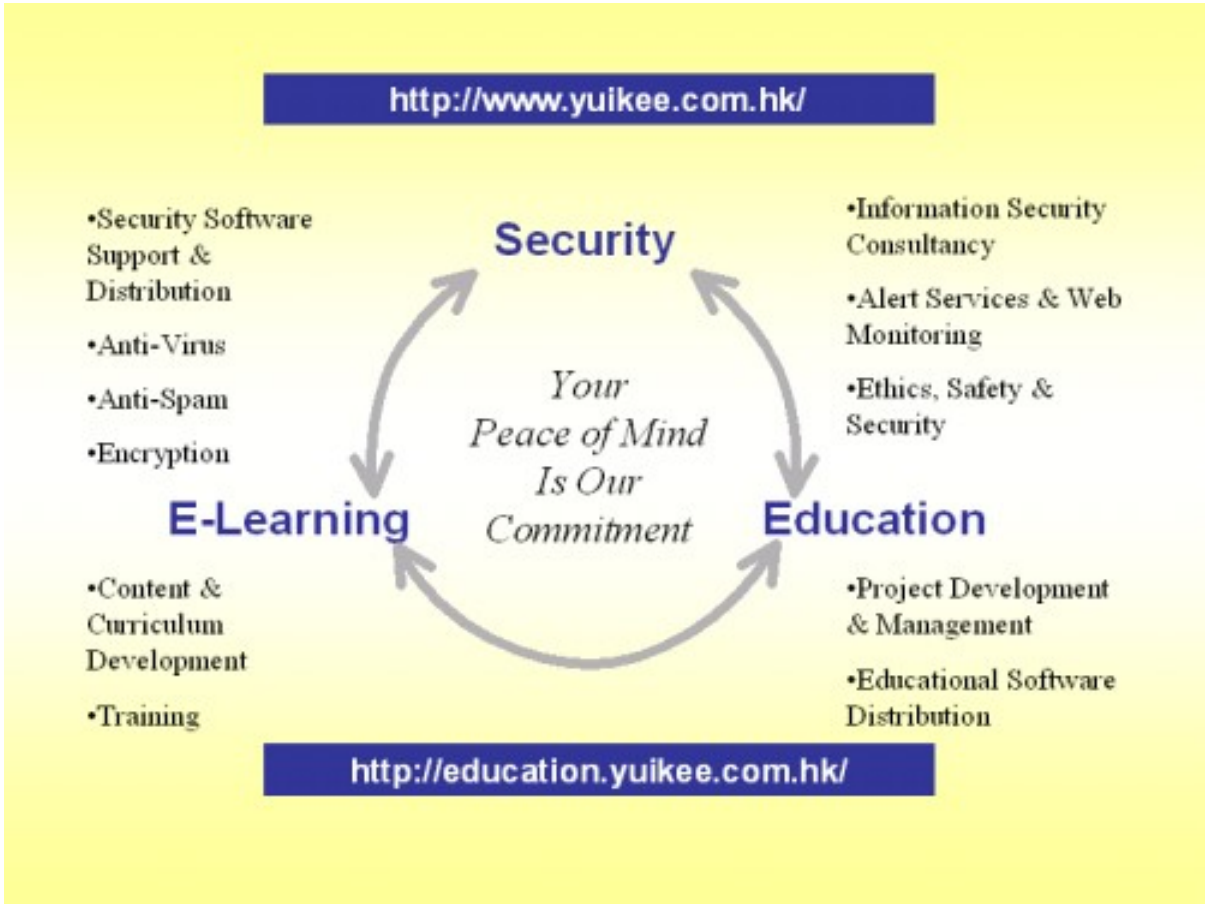
To ensure that home PCs are protected to the same level as the corporate intranet, network administrators should install the latest security patches available online, install up-to-date anti-virus software and set up a personal or distributed firewall.

It is also essential for businesses to educate teleworkers about their role in strengthening corporate security.

Fortunately, no one is going to die from a computer virus, but such an outbreak could be the last straw that breaks a company during these difficult economic times.

Allan Dyer is president of the Association of Anti-Virus Asia Researchers

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/