I am Chun. I am the owner of an innovation and technology SME.

I am Chi On, a friend of Chun's.

I am an information security consultant.

I am a hacker.
Today I am going to steal the new patent technology from Chun's company
to make profit.

Does the pandemic affect your business, Chun?

Quite badly. Our business has dropped a lot.
but thankfully no disruption to our business operations.
Nowadays, it is easy for colleagues to work and have meetings remotely.

Does remote working pose any information security risks, On?

Yes, when colleagues work remotely,
their computers are not protected by company's security measures.
There have been many cyber attacks targeting remote workers recently.
For example, hackers would send phishing emails to steal personal information
and scan for security loopholes for hacking the systems.
They may even encrypt your information with ransomware.

Haha! I tricked you into connecting to my fake Wi-Fi hotspots!
Now I can copy your files!

We are using remote desktop control software
to control our office computers via our home computers.
Would that be a problem?

The advantage of this method is easy to install.
Yet, it would bypass the company's firewall
to remotely control the office computers.
Could pose security risks by solely rely on the software's security controls.

I see. So what is VPN?

VPN is like an encrypted channel.
It protects the information transferred in between.
But if security issue already persists in the home computer,
the company's systems and data could also be affected.

Encryption?

My company’s important documents are also encrypted.

Shh, don’t share your company secrets in public.

Oh, they are encrypted! That’s why I couldn’t open them.

Actually, there are many remote working solutions in the market.
Whichever solution you choose, the most important thing is to raise employees’ cyber security awareness.
It includes…

Company should provide remote working security guidelines for employees.
require employees to use strong password
or multi-factor authentication.
Also advise employees not to connect to unknown Wi-Fi hotspots.
Companies have to review employees’ access rights regularly.
Lastly, update the system and anti-virus signature regularly.

Right, I have an online meeting shortly.
Could you give me some online meeting safety tips?

Sure. People might have overlooked the security issues of video conferencing software.
There were incidents that online meetings were hacked with inappropriate images displayed.

Wow! What should I do then?

Firstly, always use a new meeting link and password for each meeting.

Disable the “Join meeting before host” function
to ensure participants can only join after the host has started the meeting.

Use the waiting room function for the host to verify participants’ identities.

Lock the meeting immediately once all the participants have joined.

When hosting a large-scale public meeting, you should note:

First, restrict the use of audio, video and screen sharing of participants.

Second, log in as participant using another device
to check if the security settings of the meeting are working as expected

Third, enable automatic updates for the video conferencing software.

Lastly, if the meeting recordings contain sensitive information,
better store in local computers configured with proper access permissions.

Got it! Thanks for your tips.

You are welcome. I’ll leave you to your meeting, bye!

Here comes my chance!

Wow!

This can’t be right!

I am sorry, sir…

I never miss.

Can it be that my actions got discovered?

I will definitely manage to hack your computer next time!