Couldn’t hack your systems last few times.
Let me see what else I can do today!

You are quite generous, I would say,
for sharing your personal information online with everyone.

And you have liked some electronic product pages.

Let me design a phishing email to trick you!

Chun, did you tell your wife about buying the new gaming console?
That one! You know.
Its VR car racing game is exciting.

Obviously, I cannot lay my hands on one.
Everyone is crazy about it. It’s all sold out.

Awesome!
I can get the console for free by just filling in some personal information.
Let me do it now!

Hold on! Let me see.

Check here.
The sender’s email and website address does not match the company name it has claimed to be.
And there is even a spelling mistake!
The content is also very strange.
Get a gaming console for free by just filling in some personal information?
Doesn’t it look too good to be true?
It looks like a phishing email.

Nowadays, hackers are very well-planned with their attacks.
They will first make use of social media to obtain the targets’ information and interests.

Followed by a customised email or message to their targets to trick them open it.

If you have opened an attachment or clicked a link that contains malware, your systems run the risk of being infected.

Malware?

Yes!
The two most common types are ransomware and botnet.

Ransomware can encrypt the files on computers or mobile phones,
so that you cannot open them.

The hacker will then demand you a ransom for decrypting the files.

Botnet can reside on electronic device
and steal your data upon receiving the hacker's command.
The hacker can even use your device to conduct other illegal activities!

It's horrible!
How can I protect myself?

First, think carefully before opening any suspicious emails, social media messages, attachments or links.

Second, do not disclose any sensitive personal information on social media platform.
If someone asks you for sensitive information,
such as passwords or bank account numbers,
you should stay vigilant and better verify the sender's identity.

Third, do not forward or disclose your one-time password to anyone.

One more thing.
Many online services support multi-factor authentication nowadays.
Activating these functions can effectively minimise the risk of account hijacking.

Also update your systems and virus signatures regularly.
It can help you block malware.

If unfortunately you fall victim to a ransomware attack,
don't pay the ransom whatever happens.
Hackers may not necessarily decrypt the files even you pay up.

You may wish to contact the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) if you need help.

Got it!
This hacker takes advantage of my desire to buy the gaming console to trick me.
So despicable!

Don't be mad.
Let's fight back!

Form filled. Looks like I am getting you this time.

What? "Phish me if you can!"

Oh no! I fail again!