Stay Vigilant Against Phishing Emails

Polly:
Andy, I receive an email from my bank again. The email urges me to handle the account problem immediately or else my account will be frozen.

Andy:
Then, have you clicked the link in the email?

Polly:
After hearing your brief explanation of phishing last time, I dare not to click the link.

Andy:
You are a fast learner. If you follow the instructions in the email, it may lead to cyber security incidents. Let me teach you how to identify phishing emails now.

Andy:
Typically, some of the following common indicators will appear in phishing emails:

Andy:

The sender’s email address may counterfeit the genuine sender or use domains that are not officially registered by the company. In conclusion, it is not advisable to trust the email solely by the sender's email address.

Andy:
The email uses generic salutation like “Dear Valued Customer” or “Dear Member”, rather than your account name or real name.

Andy:
If you look carefully, you may notice the information in the email does not match with what you have submitted before.

Andy:
The email contains a lot of spelling mistakes and grammatical errors.

Andy:

You will be informed of winning a grand prize, making big money and any unbelievable good offer to trick you into clicking a link or opening a file attachment.

Andy:
When you hover over the link with mouse, you will find that the actual webpage address displayed by the hyperlink is different from the webpage address displayed on the screen. For example, you should note whether the webpage address should use English alphabet “l” or numerical digit “1”; or use English alphabet “O” or numerical digit “0”.

Andy:
The email will create an emergency atmosphere. For example, the email tells you that a cash-coupon will be valid for today only which will urge you to download the coupon without a thought.

Andy:
Use intimidating contents (e.g. your email account is hacked) to scare you to follow instructions to complete relevant operations.

Andy:
Last but not least, you should be aware that normal organisations will not request you to provide personal or sensitive information via email, including identity card numbers and any passwords.

Andy:
In most of the cases, both phishing emails and phishing websites will work together to cheat people.

Polly:
Andy, can you teach us how to identify phishing websites?

Andy:
Sure. Let’s talk tomorrow!

Beware of phishing emails and be careful not to open them.