Stay Vigilant Against Phishing Websites

Polly:

Oh! My online account has been stolen! It must be the phishing website that tricked me into providing personal information before. I have to follow Andy's advice to change the password immediately.

Andy:
Hold on! Have you examined the email clearly? In fact, most of the phishing emails will include links to phishing websites to strengthen credibility for stealing your information.

Polly:
How come! I think my online account was stolen and want to update my information and password by clicking the link as soon as possible.

Andy:
Cleverness may overreach itself! Phishing websites are getting sophisticated nowadays. Let me share with you some hints on how to identify phishing websites!

Andy:
First of all, check whether the website address shown in the browser's address bar is identical to that of the official website. For example, the website address of this on-line shopping site includes extra strings which indeed has no relationship with the company's official website.

Andy:
Even though a website has used digital certificate for encryption (those websites starts with "HTTPS"), it doesn't mean the website is safe. Nowadays, both phishing websites and official websites have used HTTPS.

Andy:
The contents in the website are different from those found in the genuine website.

Andy:
The website only provides direct bank transfer or cryptocurrency as the payment method, without other popular payment methods, such as credit card payment or payment portals.

Andy:
Beware of a website collecting excessive sensitive personal information.

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 "I" or numerical digit "1"; or use English alphabet "O" or numerical digit "0".

Andy:
The website contains a lot of spelling mistakes and grammatical errors. Also, the contact information is missing.

Andy:
In fact, it is not difficult to identify phishing websites as long as we pay much attention to our emails and develop good habits. For example,, instead of clicking links in an email directly, input the website address directly in the address bar of a browser. This helps you to stay away from phishing websites.

Polly:
I really have to stay alert with my personal information!

Andy:
Of course! Phishing attacks not only affect yourself, but also others!

Stay vigilant against phishing websites to keep you safe.