Phishing

Phishing

Phishing is a kind of cyber fraud. Criminals attempt to use fraudulent emails or malicious websites to lure unsuspecting web surfers to provide personal information.

Phishing Emails

Phishing emails normally involve mass distribution of 'spoofed' e-mail messages with return addresses, links, and branding which appear to come from banks, insurance agencies, retailers or credit card companies. These fraudulent emails are designed to fool the recipients into divulging personal information such as account names and passwords, credit card numbers, identity card numbers etc. by following the instructions in the emails. The information collected will then be used for other illegal activities.

Phishing Websites

Phishing websites use domain names or sub-domain names similar to those of legitimate websites. They also copy genuine looking contents or real contents such as images, texts or logos to entice visitors to enter their accounts or financial information.

Phishing emails usually entice the recipients to click on embedded hyperlinks that will direct them to some fraudulent websites instead of the genuine websites displayed.

Potential Threats

What are the potential threats you will face if you suffer from a phishing attack?

Since the phishing emails often look "official", some recipients may respond to them and click into malicious websites, resulting in disclosure of personal information, financial losses, identity theft or other fraudulent activities.

Preventive Measures

In order not to be cheated by phishing activities, what preventive measures should we consider?

- Open email attachments with care, and do not follow links embedded in emails.
- Do not visit suspicious websites or follow the links on those websites.
- Do not follow links from search engines results to log on accounts of banking or financial organisations. You should type the URL manually or follow the bookmarks you have added.
- Use 2-factor authentication, such as password plus smart card, for online banking to confirm user identity.
- After performing an online banking transaction, remember to print or keep the copy of transaction record or confirmation notice for checking later.
- Always be wary when giving off personal or account information. Banks and financial institutions seldom ask for your personal or account information through email. Consult the relevant organisation if in doubt.
- Log in your accounts regularly to check the account status and last login time to determine whether there are any suspicious activities.
- Review your credit card or bank account statements as soon as you receive them to check for any unauthorised transactions or payments.
- Furthermore, you must apply basic security measures on your computer, including installing anti-malicious code software (such as anti-virus software), firewall and latest security patches, scheduling a weekly full scan and enabling the Auto Update feature of relevant software.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk