Common Frauds

Introduction

The Internet brings us a lot of information and services. Some electronic services require user authentication, such as those involving:

- money transaction, e.g. e-banking;
- paid service, e.g. subscription to paid magazine;
- registered service, e.g. checking your information online;
- legal liability or contract terms.

However, using these e-services without caution may subject you to fraud, resulting in loss.

Four steps of common frauds

Fraudsters would

1. steal your personal information and use it as credentials;
2. impersonate your identity to log in the authentication system;
3. use your identity to conduct transactions, use services or provide electronic signature;
4. cause you direct or indirect loss to varying degrees.

Stealing Credentials and Impersonation

Fraudsters would deploy different means to steal your credentials, such as through:

- fraudulent websites;
- fraudulent emails;
- fraudulent phone calls; or

- fraudulent letters.

Fraudsters would establish a fraudulent website with fake URL or home page that looks almost indistinguishable from the genuine one (such as using www.ebank.org to fake www.bank.org), and lure you to enter the website and provide your personal information by the following means:

- Issuing urgent or alarming emails requesting you to click on the provided hyperlinks to confirm your account information;
- Using pop-up windows, making telephone calls or sending letters requesting you to provide personal information for entering lucky draw or claiming your prize;
- Providing hyperlinks in discussion forums, emails, etc. for you to click on without caution.

Subject to different requirements of the service and the authentication system, fraudsters would steal your personal information to impersonate you, such as

- user name;
- password;
- identity card number (full or part);
- credit card number;
- credit card expiry date.

<u>Conducting transactions to gain benefits</u>

Fraudsters would conduct transactions using your account or identity, such as:

- Making bank transfer or payment;
- Shopping online;
- Subscribing to services;

- Checking your account information, such as transaction records;
- Submitting documents with electronic signature;
- Accepting terms under your user name.

These transactions would cause you direct or indirect loss to varying degrees, such as money loss, data leakage, liability.

Tips

To avoid frauds, we need to be on alert at all times. Here are some suggestions:

- Use bookmarks for important or frequently visited websites to ensure the correctness of URL;
- Avoid clicking on unfamiliar hyperlinks, and carefully verify the websites to which these hyperlinks direct;
- Avoid disclosing you credentials or sensitive personal information to anyone or through electronic channels, unless you have verified their identity;
- Keep abreast of fraud news and cases, such as news about fake websites published by the Hong Kong Monetary Authority, to better understand fraudulent practices.

Conclusion

Stay Alert, Avoid Frauds