Common Threats (Identity Theft)

Introduction

Electronic identity is widely used for electronic transactions (e-transactions). While electronic identity helps to build trust and ensure e-transactions are conducted in a secure manner, its improper use could result in more threats to users as fraudsters will make use of the loopholes in e-authentication process to obtain user information.

Registration

Fraudsters may use your personal information to impersonate you to perform registration. They can obtain your personal information in the following scenarios:

- You perform registration and provide unnecessary personal information in fraudulent websites inadvertently;
- You have disclosed your personal information to other people or organisations, who use your information improperly without your permission.

If you receive an email, SMS or letter stating that you have registered for or used a particular service, which is not the case, it means someone might have impersonated you. To rectify the situation, you should:

- Report to the service provider about the abnormality and revoke the account immediately;
- Check out how the service is registered and what transactions have been conducted;
- Check out your loss or liability and negotiate with the service provider on the responsibility issue;
- Report to the police for assistance where appropriate.

Authentication

Fraudsters may use your account and credentials to conduct e-transactions under your name. They can obtain your credentials through the following ways:

- Peeking: fraudsters may peek over your shoulder to obtain your username and password;
- Password guessing: fraudsters may use some password guessing tools or techniques to try your password;
- Terminal access: fraudsters may obtain your information via the terminal you have just used but forgot to properly log out;
- Fraudulent websites: fraudsters may obtain your account information and credentials via fraudulent websites; or
- Loss of token: fraudsters may find your lost token or mobile phone, through which they can obtain your one-time password.

If transactions or login activities that are not conducted by you are detected, it means your identity may have been stolen and used by others. To rectify the situation, you should:

- Report to the service provider about the abnormality and revoke the account immediately;
- Check out what transactions have been conducted;
- Check out your loss or liability and negotiate with the service provider on the responsibility issue;
- Report to the police for assistance where appropriate;
- Create another account or change the password where appropriate.

Tips

To protect your electronic identity, you should:

- Protect your personal information properly, and never disclose it to others

casually;

- Do not authenticate to or log in your subscribed electronic services via public terminal (e.g. those provided in coffee shops or libraries) or unsecured terminal;
- Ensure log-out after use;
- Choose a password which is easy for you to remember but difficult for others to guess;
- Check the authenticity of websites, and never provide sensitive or account information in websites from unknown sources.

Conclusion

Protect Identity, Avoid Thefts