# Good Online Practices

## Introduction

You may go online almost everywhere, e.g. at home, at public places or through mobile devices. In the following example, Arthur shows you some good online practices.

## 1. Use Secured Terminal

Arthur wants to make transfer via e-banking in a coffee shop. For security reason, he decides to go home using his own computer instead of using public terminal provided in the coffee shop.

**Hint: DO NOT** log in such electronic services or conduct authentication via public or unsecured terminals.

## 2. Transmit Encrypted Information

Arthur uses his own computer at home. He checks if the link between his browser and the website concerned is encrypted before transmitting sensitive information via e-banking service every time.

**Hint: DO** transmit sensitive information (e.g. passwords) in encrypted format.

## 3. Check Website Authenticity

He also checks the SSL certificate of the website before login to ensure its authenticity.

**Hint: DO** check the authenticity of website.

## 4. Use Strong Password

He uses a password comprised of at least 8 alphanumeric characters and punctuations for login.

**Hint: DO** choose a password that is hard to guess but easy for you to remember.

### 5. Check Account Regularly

After login, he checks his account status, activities and login records to detect any suspicious activities.

**Hint: DO** check your account status, activities and login records regularly.

### 6. Ignore Suspicious Hyperlinks

When using online service, an instant messenger window with a hyperlink pop up. Arthur ignores messages of unknown source.

**Hint: DO NOT** click on the hyperlinks of suspicious sources.

### 7. Log Out After Use

After making transfer via e-banking, he completely log out to prevent his account from being stolen by others.

**Hint: DO** log out after use.

### Conclusion

We can learn some good online practices from the above example.

**Authentication for Online Safety**