

Good Offline Practices

Introduction

Besides demonstrating the good online practices, Arthur also shows his friend Elaine how to protect credentials when offline.

1. Keep Abreast Of Latest News

Arthur suggests Elaine to watch the news on a bogus website which appears to be used for lottery. Its actual purpose is to collect personal sensitive information for fraudulent use.

Hint: DO keep abreast of the latest news about bogus or suspicious websites.

2. Keep Password Away From Account Information

Elaine takes out from her wallet a note on which a username and a password were written, so that she can use the username and the password to login e-banking service. Arthur tells her not to do so. What she should do is to memorise a password which is easy to remember but hard to guess.

Hint: DO NOT keep your password and your account information together.

3. Keep Safe Custody Of Security Devices

The e-banking system requests Elaine to provide a one-time-password for completing the transaction. However, her hard token was left on her office desk. Arthur reminds her of the need to keep that security device in safe place to prevent it from being obtained by others.

Hint: DO keep your cards and security devices for authentication in safe custody. If lost or stolen, cancel them immediately.

4. Keep Emergency Contacts

Arthur then shows Elaine a note of emergency or loss reporting contacts. In case she loses her password, token, or detects any abnormal account activities, she should report to the relevant authorities immediately.

Hint: DO keep a note of emergency or loss reporting contacts of all your accounts.

5. Not Sharing Account

Without the token, Elaine intends to use Arthur's account to conduct the transaction but is refused.

Hint: DO NOT share your accounts / passwords with others.

Conclusion

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

Keep Your Credentials in Safe Custody