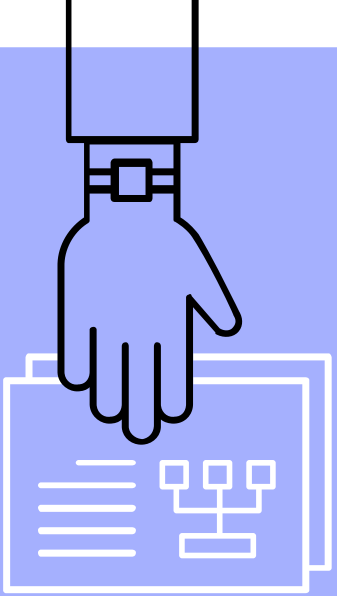
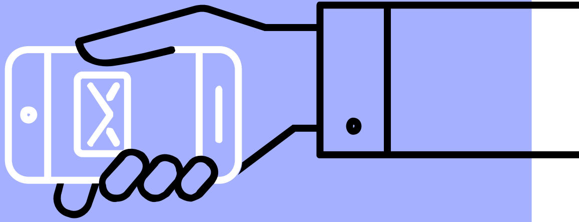
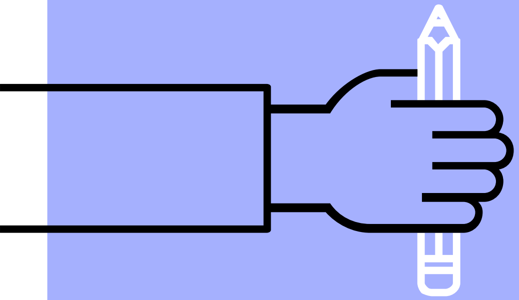
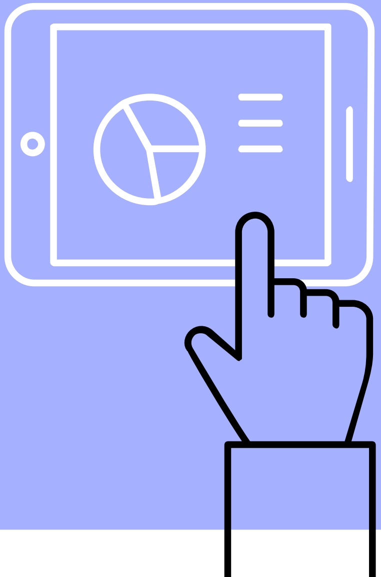




CUSTOMER INFORMATION SECURITY AWARENESS



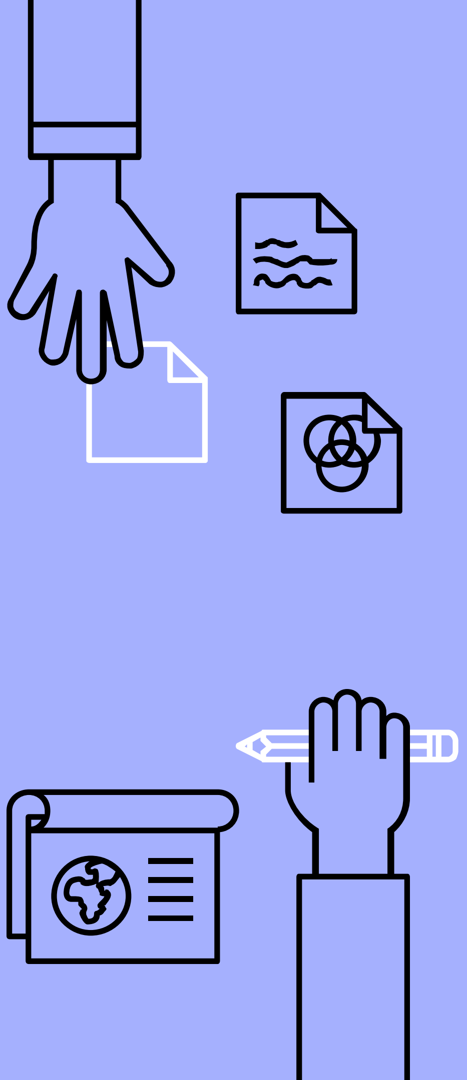


INTRODUCTION

This material is developed by Bayo Pay (M) Sdn Bhd ("Company" or "Bayo") to provide you with the basic knowledge in protecting your personal information and sensitive data from cyber threats.

In your daily activities, you may be routinely required to provide sensitive information including name, identification number and other confidential records and information as necessary to successfully carry out any transactions or services via any of our digital platform.

YOU play an important role to the defense and protection of your sensitive information as provided to any systems and data. You will be well equipped to protect your sensitive data and information by incorporating the steps and information obtained herein into your daily activities.

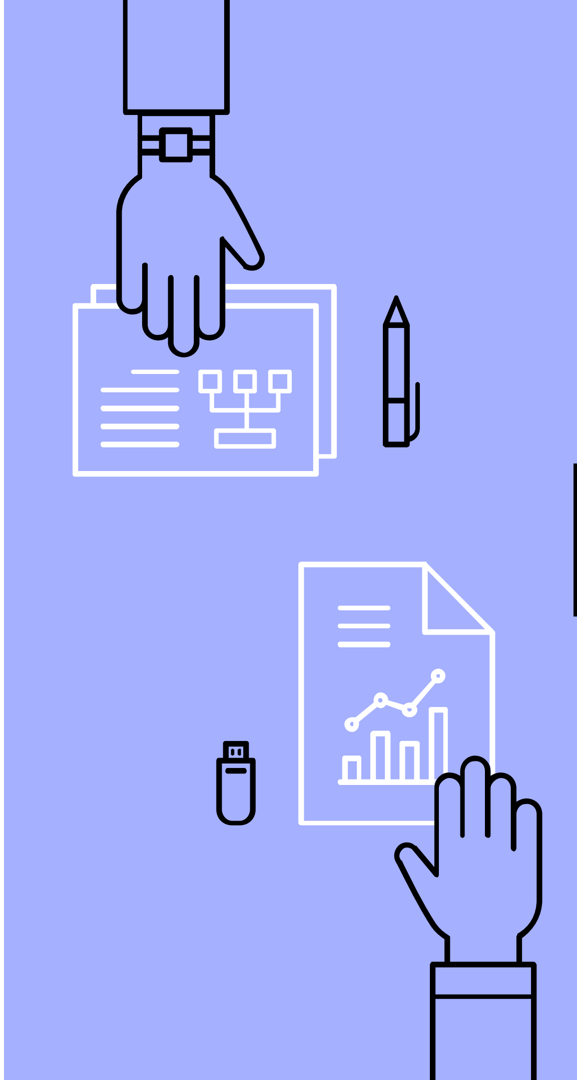


WHAT IS INFORMATION SECURITY?

Information Security (IS) – The protection of information and information systems from any unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- Information security is achieved through implementing technical, management, and operational measures designed to protect the confidentiality, integrity and availability of information.

- The goal of this Information Security Program is to help you understand, manage, and reduce the risk of cyber threats to your information while using the Company's digital platform.



THE CIA CONCEPT

CONFIDENTIALITY

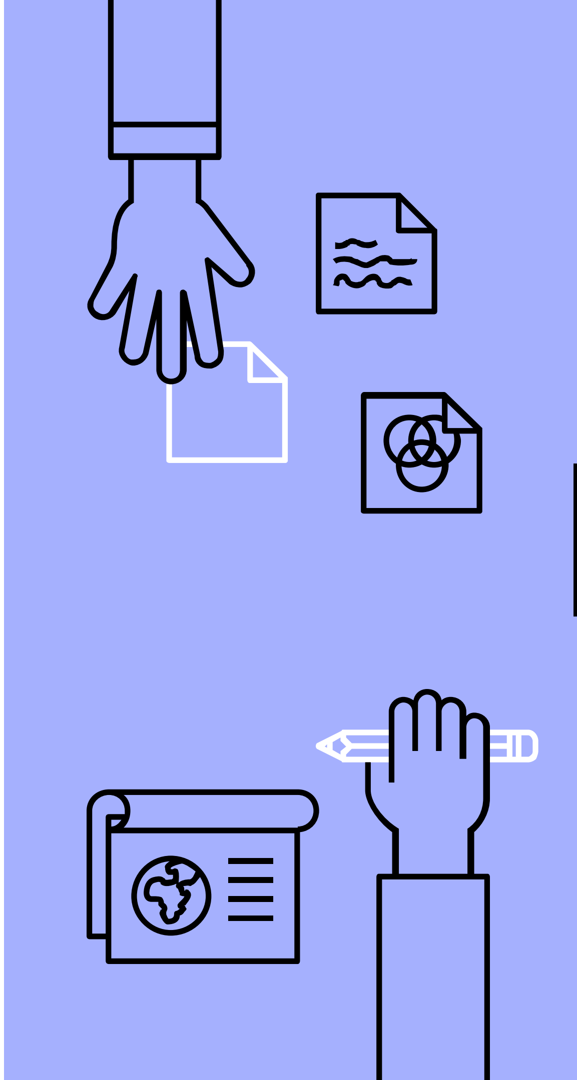
Protecting information from unauthorised disclosure to any third party or unknown or unverified source(s).

INTEGRITY

Assuring the reliability and accuracy of information and IT resources.

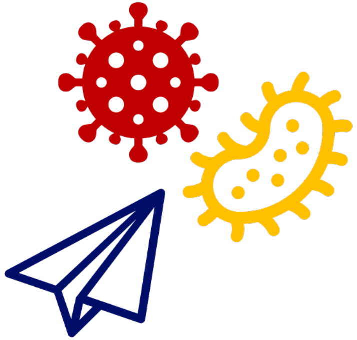
AVAILABILITY

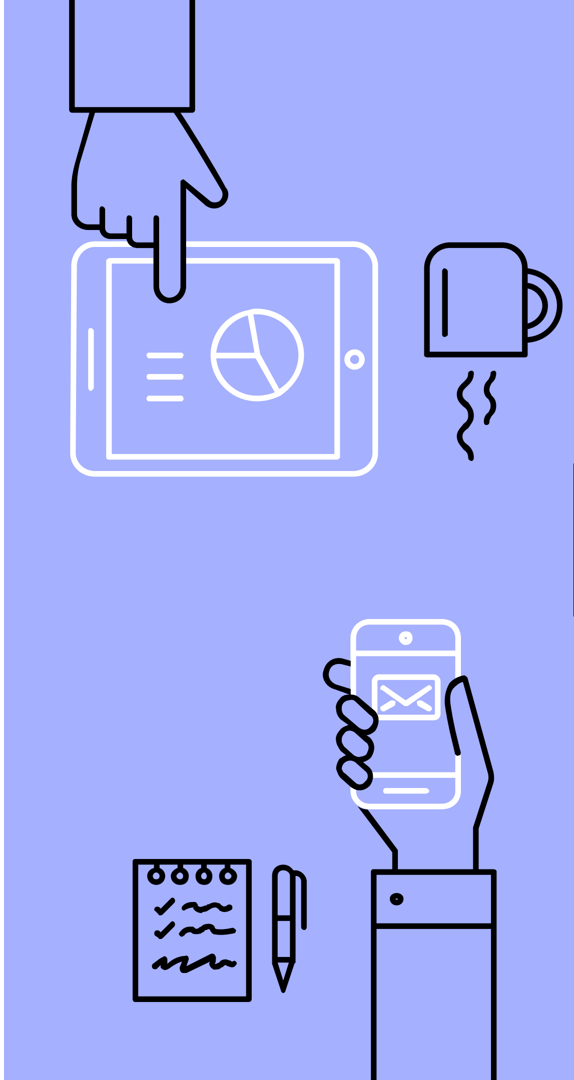
Defending information systems and resources from malicious, unauthorised users to ensure accessibility by authorised users.



COMMON CYBERSECURITY THREATS

- Viruses
- Insider threats
- Spyware
- Hackers
- Theft or loss of sensitive data
- Internet and email scams
- Phishing
- Identity theft





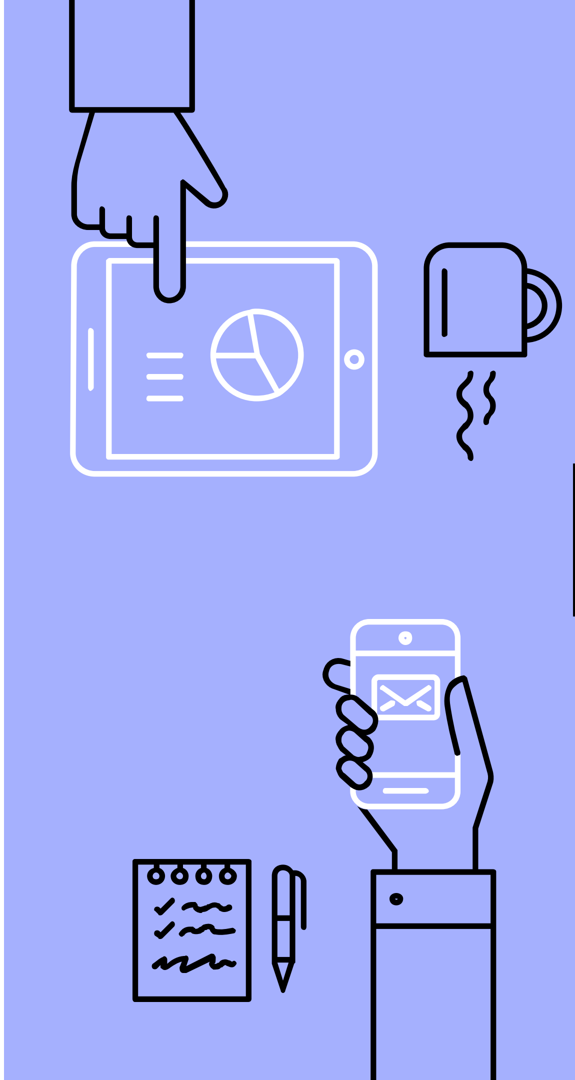
PASSWORD

A strong password for your network account and other applications is a basic protection mechanism.

- Two rules for stronger passwords:
  - a) Create a password of at least eight (8) characters in length.
  - b) Password should contain at least one combination of two or more of the following:
    - i. *Capital letter*
    - ii. *Lowercase letter*
    - iii. *Number*
    - iv. *Special character (%,^,*,?)*

- Use a passphrase.
  - a) Use the initials of a song or phrase to create a unique password
  - b) Example: "Take me out to the ballgame!" becomes "Tmo2tBG!"

- Remember and keep your password.
- DO NOT keep passwords near your computer or on your desk.



COMMON PHISHING SCHEMES TO WATCH OUT

SPEAR PISHING

Fraudsters target a specific individual or organisation. They use information particular to the recipient, usually sourced from social media accounts, to appear legitimate and gain the person's trust. Because these attacks are specific, their chances of success are generally high.

MALVERTISING

Derived from "malicious" or "advertising", fraudsters create malicious ads which aims to spread malware that would later damage the system. That way, they can get access to sensitive information.

E-MAIL

You will receive an email from fraudsters which contain a URL/link by pretending someone you trust and may perceive you to click on the link to fill in your personal details on the fake website.

The fraudsters will obtain all your sensitive information such as usernames, passwords, phone numbers, and card details to make an intentional financial transaction once the URL/link is clicked.

PHONE CALL

Fraudsters will call you to pretend that they are calling from the governmental authorities or legitimate financial institutions or organisations (i.e. Bank / FinTech / MACC).

They will pose as officers or authorised representatives of any organisation and request for your personal information / accounts / cards; and ask you to key-in your personal information immediately.

SMISHING

Fraudsters would usually send out text messages containing a phishing website to different numbers with hopes of victimising as many as they can.

For instance, a text message is sent directly to your mobile number that mentions your card has been charged on certain amount and they will provide their contact number to get more details or request for your TAC number.

ONLINE PURCHASE SCAM

Fraudsters use the latest technology to set up a fake online retailer website that seemed genuine like other online retail stores.

They will create a fake advertisement where you can click and purchase with them. Once they have received your money, you will not get the item that you purchase.

PROTECT YOURSELF

DOUBLE CHECK E-MAILS

Take a second look at e-mails from the Company. Remember that the Company will never e-mail requesting you to verify or provide your personal info.

CHECK FOR TYPOS

Check for the telltale signs of phishing, such as incorrectly spelled URLs in e-mail links and further request for personal data and confidential information.

BE CAREFUL WHEN POSTING ON SOCIAL MEDIA

Skip that social media post about your personal info. For instance, date of birth as these may be used by scammers already in possession of your log in credentials to steal your identity.

DON'T REPLY!

If you receive an e-mail from a source that you know but it looks suspicious. For instance, the e-mail was unsolicited, it contains grammatical errors, or it redirects you to another site – write that source with a new e-mail, instead of just hitting reply.

DO's	DON'Ts
Download our official Application from Google Play Store, Apple App Store and Huawei AppGallery with verified marks.	Put the Bayo Pay link as a bookmark or favourite in your search engine.
Login to Bayo's site by typing the correct URL into your browser.	Use the public network for any financial transaction.
Disable auto-save functions for username and password.	Reuse passwords and keep passwords on the mobile device.
Check log in details activity frequently and monitor any suspicious login attempts.	Use generic information that can easily be obtained like birth dates, phone numbers, vehicle information, etc.
Change passwords regularly and create a different password for each system or application.	Share your login ID, password or TAC with anyone and reveal your personal details, etc.
Install updated anti-virus software and only use trusted WIFI's or network service provider.	Click on an unknown website link or open attachment sent via emails, SMS pop-ups or Social Medias.
Encrypt all devices which contain sensitive information.	
Check your transactions record regularly.	

CONTACT DETAILS

All notices, requests and/or other communications to BPSB must be communicated to the following address :

Customer Service Department
Bayo Pay (M) Sdn Bhd
No. 72-3, Jalan PJU 5/22, Encorp Strand,
Pusat Perdagangan Kota Damansara,
Kota Damansara PJU5,
47810 Petaling Jaya, Selangor.
Tel. No. : 603 – 7621 5151 Fax No. : 603 – 7662 1264
E-mail : support@bayo.my

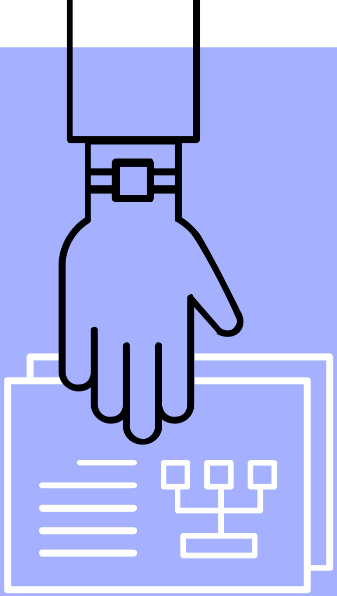
CONTACT DETAILS

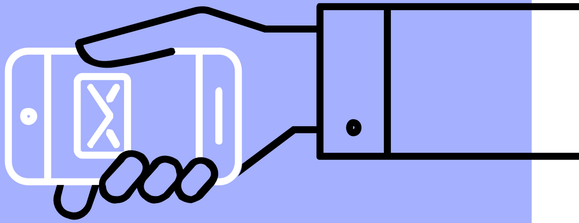
If there are complaints or inquiries, you may contact the following bodies :

Bank Negara Malaysia
Laman Informasi Nasihat dan Khidmat (LINK)
Ground Floor, D Block
Jalan Dato' Onn
50480 Kuala Lumpur

Contact Centre (BNMTELELINK)
Tel No. : 1-300-88-5465 (Foreign : 603 – 2174 1717)
Fax No. : 603 – 2174 1515
Email : bnmtelelink@bnm.gov.my

Ombudsman for Financial Services
14th floor, Main Block
Menara Takaful Malaysia
No. 4, Jalan Sultan Sulaiman
50000 Kuala Lumpur





THANK YOU