Article Series: Be Protected by Being a Responsible Financial Consumer Online
Part 1

As technology in financial services has evolved, so have its risks. Recently, there has been an increase in smartphone malware scams, phishing messages, and online payment fraud in the region and also in Brunei Darussalam. To tackle these cyber threats and protect their customers, financial institutions continue to take steps to strengthen their banking systems and avoid data breaches.

At the same time, consumers like you also play a major role in keeping your personal data safe and in securing your devices. With both financial institutions and consumers working together, we can build a strong defence against the risk of information theft and financial loss, and stay safe online.

In this 4-part series of articles, we share some tips and advice on how to increase protection against digital fraud by being a responsible financial consumer online. This week, we will talk about how to protect your personal data.

1. Protect your personal data

Personal data refers to details that can be used for identification or verification purposes. This includes your full name, date of birth, identity card number, phone number, residential address and e-mail address.

DOs

- Always check with your bank through their official communication channels to verify whether a call claiming to be from a bank is legitimate.

DON'Ts

- Never disclose your personal information or data over the phone or social media. This could be used for identity theft.
- Avoid sharing personal information and images over social media that can allow malicious individuals to learn more about you without your consent and to gain access to your personal data.

Other information that you should always keep safe to avoid unauthorised access or misuse by other individuals include:

- Bank account number;
- Credit or debit card number including the expiry date, and CVV code;
- Internet or mobile banking details e.g., username and password;
- Any online accounts used for shopping or as e-wallet;
- Travel plans and boarding passes (barcodes can reveal personal information);
- Receipts or invoices, especially with QR codes;
- Information contained on shipping labels for online purchases; and
- Names of immediate family members.

Did you know?
If you give or share access to your mobile phone number, bank account or debit card with someone else, you could be unknowingly involved in illegal activities and charged with assisting in money laundering, which is a criminal offense under Section 3, Criminal Asset Recovery Order (CARO), 2012.

If found guilty, you may face a fine of up to B$500,000 or imprisonment for a term not exceeding 10 years.

So, be careful and never give away your personal information to anyone you do not know and trust.

2. Safeguard physical items containing sensitive information

It is important to make sure that anything physical that contains sensitive information is kept safe. In today's world, both digital and physical assets are at risk of being targeted by people with malicious intent. Examples of these items include:

- Bank account passbook;
- Credit and debit cards;
- Mobile phones, tablet devices, laptops, or any device used to make financial transactions; and
- Authentication tokens or devices issued by your bank.

DOs

- Properly dispose of and destroy any documents containing sensitive financial information, such as bank statements, receipts, expired credit and debit cards, and shipping labels.

DON'Ts

- Never leave physical items that contain sensitive information unattended, even for a short period of time. Always keep these items with you or in a secure location.

These simple practices are designed to empower you with the right tools to keep your financial information and transactions safe.

Catch the next article in this series next week for more tips and advice to protect yourself online!

This series is a joint initiative brought to you by:
Brunei Darussalam Central Bank (BDCB) (Instagram: @centralbank.brunei),
Authority for Info-communications Technology Industry of Brunei Darussalam (AITI) (Instagram: @aiti.brunei),
Cyber Security Brunei (CSB) (Instagram: @csb.gov.bn), and
Brunei Association of Banks (BAB) (Website: www.bab.org.bn)