

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 more about securing your devices and the importance of being aware of risks associated with digital transactions or applications such as cyberattacks, online fraud or scams, and personal information theft.

1. Secure your devices

Securing all the devices which you use to make financial transactions helps protect your personal and financial data. Individuals often fall victim to unintentional downloading of malicious software after clicking on links from unknown sources. This can result in their banking information being stolen or unauthorised access to their bank accounts.

DOs

- Regularly update operating systems, applications and/or firmware on your devices.
- Only install applications from official application stores such as Apple AppStore or Google Playstore.
- Remove any unnecessary or unused applications on your devices.
- Check the applications on your phone to ensure that no unknown applications have been installed.
- Disable features like wireless, Bluetooth, and Near Field Communication (NFC) when not required.

DON'Ts

- Do not click on unknown or unverified internet links. Scammers use attractive click-bait titles and images to interest you into clicking on links that may contain malware.
- Avoid jailbreaking or rooting your smartphone.
- Avoid plugging into unknown USB ports or devices.
- Never accept any suspicious activity on your smart device that triggers a warning.

2. Always be aware

In today's digital age, it is important to always be aware and vigilant. Whether you are accessing or discussing your information in a public space, or browsing the internet and making online purchases, it is crucial to always be aware of the potential risks and take steps to protect yourself. By remaining aware and proactive, you can significantly reduce your risk of falling victim to cyberattacks.

DOs

- Discuss financial matters in private settings where there is less chance of eavesdropping.
- Exercise caution when making payments at any shop premises or using ATMs in secluded locations.

- Be aware of your surroundings when entering account details and be cautious against prying eyes.
- Ensure the web address or URL for banks and online shopping begins with 'https' or have a closed lock icon.
- Double check the details of the website you visit because hackers use visually similar characters to deceive people.

DON'Ts

- Avoid making online transactions on websites which seem dubious or are not familiar to you.
- Avoid online transactions on open or unsecured public Wi-Fi, including fake wireless hotspot.

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)