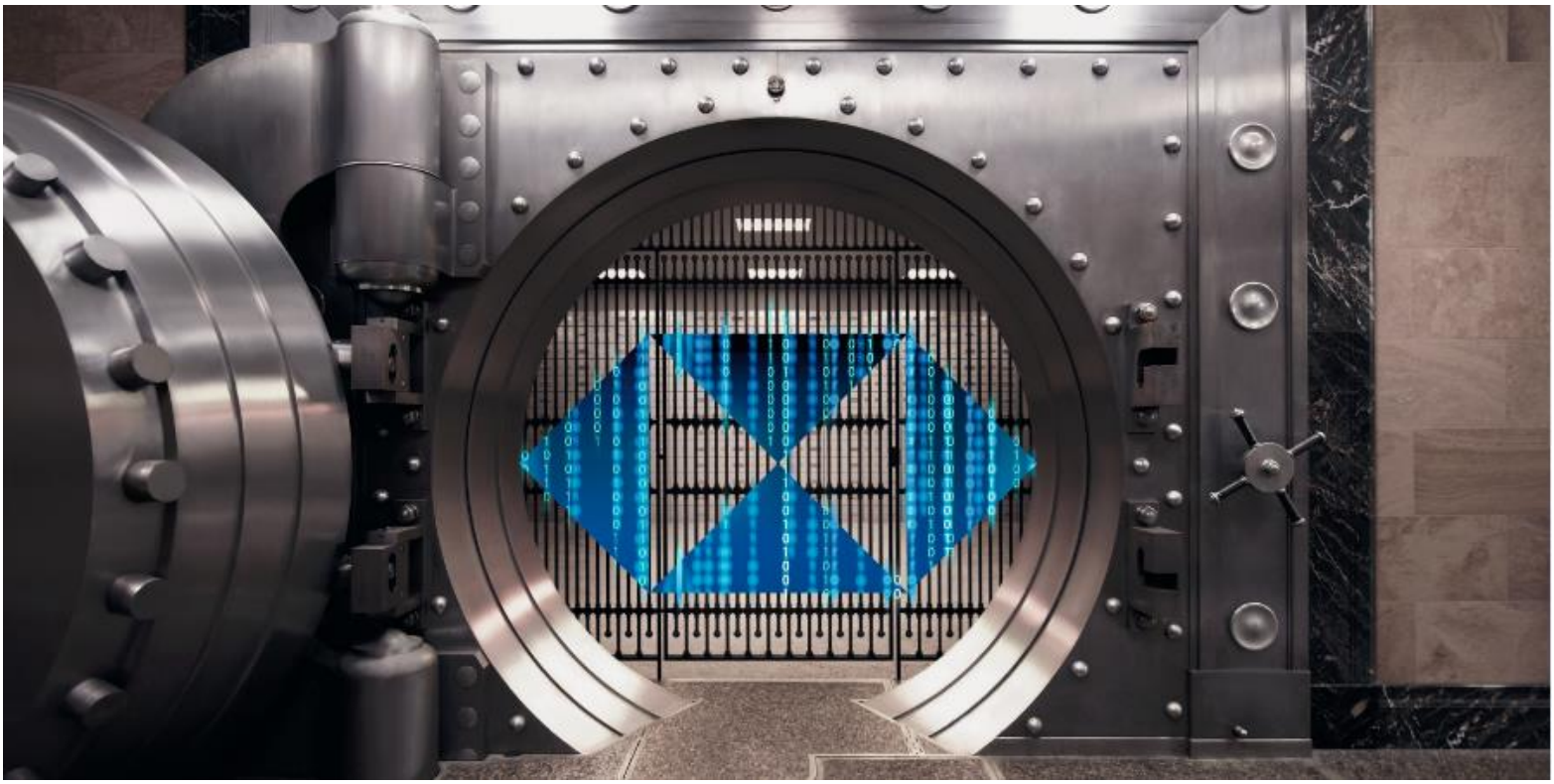

#BEcyberSmart to #BEcyberSafe

Don'ts

- DON'T post any private or sensitive information, such as credit card numbers, passwords or other private information on public websites including social media sites, or even through emails.
- DON'T click on links from an unknown or untrusted source.
- DON'T be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner.
- DON'T respond to phone calls or SMSs requesting confidential data.
- DON'T install unauthorized programs on your home or work computer. Malicious applications often pose as legitimate software.
- DON'T leave devices unattended, especially in public places.

- DON'T purchase anything promoted in a spam message. Even if the offer isn't a scam, you are only helping to finance and encourage spam.

- DON'T open an e-mail attachment, even from someone you know well, unless you were expecting it.
- DON'T reply to e-mail(s) requesting financial or personal information.

- DON'T give any personal information, card details and personal identification details to an unknown caller.

- DON'T give your credit card number(s) and CVV numbers online unless the site is a secured and reputable site.

- DON'T make passwords that includes any personal details.

DO's

- DO create strong passwords that are at least eight characters long, and including at least a numerical value and a symbol such as #.

- DO use different passwords for different accounts, so that If one password gets hacked, your other accounts are not compromised.

- DO keep your passwords confidential.

- DO pay attention to phishing traps in email and watch out for red flags of a scam. If you receive a suspicious email, the best thing to do is to delete the message.

- DO inform the Bank if you feel suspicious or if you feel your email, personal information, credit card information is compromised.

- Avoid using public Wi-Fi hotspots.

- DO Download and install software only from online sources you trust.

- DO Close windows containing pop-up ads or unexpected warnings by clicking on the "X" button in the upper top right hand corner of that window, not by clicking within the window.

- DO Use an antivirus software and update it on a regular basis to recognize the latest threats.

- DO Regular updates to your personal computer’s operating system, web browser and other major software using the manufacturers' update features, preferably using the auto update functionality.
- DO your homework on the individual or company to ensure that they are legitimate when any form of contact is made.

- DO Make sure you are purchasing merchandise or paying for a service from a credible and legitimate source.

- DO Check your online accounts, bank statements, bank SMS alerts regularly.

- DO Educate yourself, your loved ones, about potential threats and scams. Teach them to hang up on an unsolicited call and directly call the person, department, or company using the official phone numbers (such as from an official directory or from official web site.)

- Keep all mobile devices, such as laptops and cell phones physically secured.