CTBC BANK
中國信託銀行

Cybersecurity

We understand cybersecurity is important to you; that is why Protecting your privacy and safeguarding your personal information is a cornerstone of our organizational ethics and values and will always be one of our highest priorities.

In an age where we manage more and more of our lives digitally, it means that anyone should know simple things about keeping security up to par. At work, this will help companies maintain robust protocols. At home, it will help you protect your own information.

The followings are a few reminders on how you could do to protect yourself in the digital age,

Be cautious of emails, phone calls and websites that promise incredible deals and monetary windfalls. If it sounds too good to be true, it probably is. The results of these scams can end up unauthorized withdrawals from your bank account or credit card, identity theft, fraud, computer viruses etc.

Always keep your personal information, like Personal Identification Number (PIN), password etc. safe and confidential. Do not give them out on the phone, through email or the Internet unless you initiate the contact and know who you are dealing with. When conducting a transaction, shield the keypad when entering your PIN and look out for shoulder surfers. CTBC Bank Canada will never request your PIN or Social Insurance Number in an unsolicited email or phone call for any reasons.

Do not use your birth date, phone number, address or simple combinations as your password. Make it difficult to guess but easy to remember, like a combination of upper and lower case letters, numbers and symbols. Don't write in down or keep it in your wallet or purse. Change your password and verification question regularly. Turn off features that automatically save passwords.

Log off from Internet Banking and close your browser when you have finished your online banking session. Clear your browser's history and cache on a regular basis. Avoid accessing your online banking information at Internet or Cyber cafes, libraries or other public Internet portals Be careful about including personal information online, on social networking sites, in chat rooms and in unencrypted email.

Email fraud : "Phishing"

What is Email fraud?

Internet scammers casting for peoples' financial information have a new way to lure unsuspecting victims: They go "phishing". Phishing is a high-tech scam that uses spam or pop-

up messages to deceive you into disclosing your credit card numbers, bank account information, Social Insurance Number, passwords, or other sensitive information.

How does it work?

Phishers send an *email* or *pop-up message* that claims to be from a business or organization that you deal with - for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To *trick you into divulging your personal information* so the operators can steal your identity and run up bills or commit crimes in your name.

How to protect yourself against email fraud?

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. Use encryption software to protect wireless devices like laptop or cell phone.
- A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband

connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- Be cautious about opening any attachment or downloading any files from emails you received, regardless of who sent them.

Where to report the email fraud?

If you believe your confidential information may have been stolen or obtained by a fraudulent party either online, by telephone or through any other means,

Contact your branch or call us at 604 683 3882 immediately

If you think you are a victim of identity fraud

- Contact the Royal Canadian Mounted Police Canadian Anti-Fraud Centre
- Request a copy of your credit bureau report and review for anything that is not yours.

- Contact Information:

Equifax	1-877-323-2598	www.equifax.ca
TransUnion	1 877 525 3823	www.tuc.ca

Please review your Online Banking Agreement for personal account or Direct Services Agreement for business account for more information about your rights, risks and responsibilities.

Management

CTBC Bank (Corp.) Canada