Cyber Security- Useful Tips & Advisories

Cyber-Security useful tips and advisories are guidelines intended to all CL clients in order to assist them in safeguarding their Data assets. It provides an overview of the technical security measures that should be adopted to protect information, data, systems and resources from any misuse or damage.

In addition, these tips provide the basic information security concepts to build a solid foundation on how to implement the security measures and maintain information security during daily operations or transactions.

1. LOGON IDS & PASSWORDS

The access to CL online banking requires a user account (username and password combination) which it will be provided by the Bank.

1.1. Creating a Password

After the first successful logon, it is essential and imperative that you change the assigned password. You have to carefully choose a good password and keep it confidential.

Find below some guidelines that help you create strong passwords you can remember:

- Do not use names;
- Do not use family names;
- Do not use personal information (e.g.: your date of birth);
- Do not use words that appear in dictionary;
- Do not use your logon ID;
- Use a password of at least eight characters, including a combination of upper and lowercase letters and numbers.

1.2. Using logon IDs and Passwords

- Keep your password confidential;
- Change your password if you think it has been compromised;
- Never let others use your logon ID or password and don't use theirs; and,
- Do not write down your password or reveal it to anyone.

2. ACCESSING CL ONLINE BANKING

Accessing CL online banking should be limited to the following approaches:

- You enter the url of CL online banking- https://ecl.com.lb; or
- You access it from CL main homepage- http://www.creditlibanais.com.lb

These practices ensure that you are entering the legitimate site and not a fake. In addition, it is highly recommended to access CL online Banking from systems/devices owned by you and from trusted Internet hotspot- avoid the use of free Wi-Fi and hotspots.

3. PROTECTION AGAINST VIRUSES AND MALICIOUS CODE WORMS, TROJAN HORSES, TRAP DOORS

Viruses and other forms of malicious code are harmful software that can contaminate, damage, or destroy information resources. Viruses can attach to e-mails, reproduce themselves, and spread automatically from computer to computer, causing widespread damage.

Symptoms of infection include:

- Files or data suddenly unavailable;
- Unexpected processes, such as e-mail transmissions self-start;
- Files have been edited, though no changes have occurred;
- Files appear or disappear, or undergo unexpected changes in size;
- Systems display strange messages or mislabel files and directories; and,
- Systems become slow, unstable, or inaccessible.

3.1. Preventing Infection

Make sure your workstation and any portable and home computers you use are equipped with virus protection software having the latest virus scanning pattern recognition file and the security patches of the operating are installed. Additional measures should be taken as follows:

- Scan diskettes and removable disk drives before using them;
- Scan incoming files before you load or save them to your computer;
- Scan files from an un-trusted source before sending them to another Computer on the network;
- Do not download unapproved programs, shareware, or freeware from the Internet, diskette, or other media;
- Do not open unsolicited or suspicious e-mail or attachments;
- Do not disable automatic virus scanning programs

4. PHISHING ATTACKS

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. **Phishing emails may contain links to websites that are infected with malware.** Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users.

Subsequently we would like to draw your attention that you might receive a deceiving email **as if originated from Credit Libanais** requesting from you to:

- Provide your credentials: username and password;
- Hit on a link for a website with promises to certain financial gain;
- Information about your organization;
- Information about your financial status
- Or others.

We urge you to ignore and disregard such email and contact Call Center.

Please be advised that Credit Libanais will never ask **you to update your information via email**