CARIBBEAN
CONFEDERATION
OF CREDIT UNIONS

Protecting Credit Unions against Fraudulent Activities

Introduction

The novel coronavirus (COVID-19) and its resulting effects has been forefront on the minds of most of our members and employees for the past few weeks. As such, our members are now more concerned and anxious about their health and safety. Credit Unions (CUs) have to be prepared for these new economic times and make the necessary changes to navigate these unprecedented waters.

As CUs begin to adopt work from home policies, this rapid shift has opened up threats related to increased crimes and more specifically an increase in laptop crimes. These cyber-attacks not only target our members but also our employees as well. The Management teams at all CUs bear the responsibility of ensuring that all employees comply with the provisions provided and ensure that a written security program for all CUs and branches is developed and implemented.

In this critical time, CUs must have a heightened sense of accountability and set clear standards of how security risks will be mitigated in the new working environment. It is important to reinforce the policies on security and set good examples. The following are recommendations that guide the online usage of employees: -

Cyber Security

- Understand the threats to CUs. Work with your IT teams to identify a likely attack as a result of employees working from home and prioritize the protection of sensitive information. Identify the possibility of shifting to cloud infrastructure.

- Provide clear guidance and encourage communication**:** Employees should be encouraged to communicate with management and IT personnel about any suspicious activities. Ensure that home working policies are clear and easily understood and that employees remain hyper vigilant in their daily operations.

- Provide the right security capabilities: CUs should ensure that adequate security is extended to all remote environments.

- Maintain strong passwords. Complex passwords should be used where possible. Passwords should be changed frequently to prevent any intrusions.

- Update systems and software. Updates should be installed in a timely manner including on mobile devices or any other device used for work. Communicate regularly with your IT personnel to ascertain that the latest updates have been conducted.

- Ensure that your WIFI access point is secured. To reduce the potential impact of an attack, CUs should change their default settings and passwords frequently.

- Be aware of scams: Avoid clicking on phishing e-mails, malicious domains and fake apps. Verification of emails is recommended prior to trusting the source. Scammers use these types of tragedies to exploit persons at their weakest.

- Contemplate using a VPN (Virtual Private Network). VPNs can help to create a trusted connection between employees and their organizations and ensure ongoing access to work tools. VPNs provide additional protection against phishing and malware attacks.

- Avoid using your work devices for your own personal matters. Avoid installing any apps or services that you would not do while you are at the office. If using your personal computer for work purposes, ensure that your emails are encrypted

- If using your personal computer for work, ensure that work related emails are properly encrypted and that the correct software is downloaded to protect from cybersecurity vulnerabilities.

- Encourage your IT personnel to secure work from home systems and implement incident response tools to ensure that that no harmful information has not been downloaded unto the computer.

Physical Security

- Ensure that proper surveillance systems are installed and cameras are angled appropriately to capture all movements. Recordings should be checked on a daily basis to confirm that they are operational. For CUs that can afford to install metal scanners this can be considered.

- Educate all employees on the opening and closing procedures and policies. Employees should be advised to report any suspicious activity immediately.

- Confirm that all employees are trained to use bait money, dye packs or electronic honing devices in the event of a robbery. Access gates to teller areas should be kept closed during working hours.

- Enforce the rules of members not being allowed to enter the CU premises with hats and dark glasses.

- Ensure that all credit unions are equipped with vaults that include telephones and alarms to enable employees to signal for help if locked in. Dual control should be maintained over safe combinations and vaults and the access gates to the vault area should be kept closed during working hours.

- Communicate the fire and safety procedures to all employees and ensure that regular drills are conducted. Adequate fire extinguishers should be installed in accessible areas.

Let us continue to make a difference in the lives of our members in 2020.