National Computer Board

CERT-MU

CERT-MU Security Alert

COVID-19 Lockdown: Beware of Scams

Issue Date: 22 April 2020

CERT-MU has noted an increase in the number incidents related to scams that are being reported on the Mauritian Cybercrime Online Reporting System (MAUCORS). Cybercriminals/scammers are taking advantage of the Lockdown situation and tricking people into divulging personal information, including banking details. As a result, many people are becoming victims to these scams and are losing money. The purpose of this security alert is to inform the cyber community and citizens on the different types of scams and also highlights the measures that they can take to be safe from these scams.

The following are examples of scams that are targeting people during the COVID-19 Lockdown period:

1. **Robocalls /Phone Scams**

Scammers are calling mobile users on Viber and WhatsApp and posing as employees of a particular bank and asking them about banking details such as Bank Account Number, Credit Card Details, PIN Code, whether they are using mobile banking applications. Mobile users may see the logo of the bank appearing on the mobile screen when they receive the call. Users may think that it is the bank which is calling.

2. **Lottery Scams**

Mobile users are receiving calls from unknown or international numbers, stating that they have won a lottery of Rs. xxxx amount. Users are requested to reveal their banking details so that the lottery amount could be transferred to their account.

3. **Medicare scams**

Scammers might call to offer services such as medicare benefits or medical checkups. To offer the service, they will ask for payment to be effected first.

4. **Grants/ Relief payment messages from government agencies**

Fake calls, texts or emails can be received from scammers pretending to be government agencies. These fake messages might state that users may receive money from the government as cash grants or quick relief payment due to the coronavirus.

5. **Faketortion or Webcam extortion emails**

In this scam, the recipient receives an email which states that the scammer holds information about the recipient such as passwords of online accounts, Facebook friends, which adult websites the recipient has been visiting, intimate pictures, amongst others. It is a blackmail email where recipients are asked to pay money to the sender or they will circulate video footage of the recipient in compromising positions. These emails also threaten the recipient that they will post/share their videos of they do not pay the ransom.

6. **Fake Online shops / Website/ Facebook page**

Scammers are taking advantage of the lockdown period to create fake website/Facebook pages to supposedly sell stuffs online with the aim to trick people and steal money. They are pretending to be well-known supermarkets/hypermarkets in Mauritius and are offering online buying services. When people are ordering online, they take the order and request for payment before delivery. Many people made the transfer and delivery is never made.

7. **Coronavirus Charity Scams**

Many charity organisations are requesting for charities to help people in distress that have been impacted by the COVID-19. Unfortunately, there are also fake charities that are popping up. They use the same tools that legitimate charities use such as sophisticated websites, emails, phone calls to trick people. They also use the names that are similar to real charity organisations.

Be Safe from these scams

CERT-MU recommends the following precautionary measures to be safe from these scams:

- Do not respond to calls or texts from unknown numbers, or any others that appear suspicious.

- Never share your personal or financial information via email, text messages, or over the phone.

- Be cautious if you are being pressured to share any information or make a payment immediately.

- Scammers often spoof phone numbers to trick you into answering or responding. Remember that government agencies will never call you to ask for personal information or money.

- Do not click any links in a text message. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they were not hacked.

- If you are unsure if an email, text or any other communication is genuinely from a legitimate source, do not click on the link or open the attachment. Contact the organisation via their official contact channels and ask.

- Protect your passwords and login credentials, do not enter these into any websites relating to the COVID-19 virus.

- Keep your devices up-to-date.

- Keep your anti-virus up to date and run regular checks.

Report Incidents

Let us unite together for a Safe Mauritian cyberspace during this crisis situation. In case you become victim to a scam, report the incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org).**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
National Computer Board
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org