Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 11 December 2025

Be Cyber Cautious During the Festive Season

Severity Level: High

Description:

As a proactive measure, CERT-MU wishes to alert the public ahead of the festive season, particularly the Christmas and New Year period, which typically sees a surge in online shopping and digital activity. During this time, cybercriminals frequently take advantage of increased online activities by launching scams, fake promotions, phishing campaigns, and fraudulent websites designed to steal personal or financial information. With many users searching for gifts, deals, and other online services, CERT-MU urges everyone to remain vigilant, secure their devices and internet connections, and verify the authenticity of any online offer before engaging with it. Examples of scams which users may encounter are as follows:

1. **Flash sale alerts**

During the festive season, users are likely to receive a number of promotional emails, including flash-sale emails. With that in mind, scammers are likely to imitate legitimate offer emails and websites to trick users and steal personal and sensitive information.

2. **"Free" gift cards or e-Cards**

Gift cards are prevalent during the holiday season. Scammers often send gift cards or e-cards containing hyperlinks via email, posing as popular online retailers such as Temu, Amazon, eBay, or AliExpress, to harvest users' credentials, such as usernames or passwords, for online accounts.

3. Fake “missed delivery” notices

The festive season is a peak time, and deliveries are often delayed. Cybercriminals take advantage of this situation and send fake “missed delivery” notices from delivery services companies such as DHL, FedEx or USPS, amongst others. These missed delivery notices look as if they are intended just for you, but they are not. The fake notices may also have a reference number to make it genuine. Those reference numbers are usually the same on each notice and may correspond to a particular offer the scammers are looking to push.

4. High Discount Offers

Users may also receive emails with high-discount offers on expensive products. For example, users may see an advertisement or email for a high-ticket item that is suddenly discounted to less than 10% of the regular retail price. These emails may contain links or malicious attachments to trick users for the purpose of stealing personal information, including banking details or online accounts credentials.

5. Robocalls /Phone Scams

Robocalls or phone scams are another popular scam during the festive season. As people shop online, they use their credit cards to make payments. Scammers take advantage by calling mobile users on Viber and WhatsApp, posing as employees of a particular bank and asking for banking details such as Bank Account Number, Credit Card Details, and PIN Code. Mobile users may see the bank’s logo on their screens when they receive the call. Users may think the bank is calling.

6. Fake Online shops/websites/ Social Media pages

During the festive season, there are fake websites or social media pages to supposedly sell stuff online with the aim to trick people and steal money. They pretend to sell things at low prices, and when people order online, they are asked to pay before delivery. Many people make the transfer, but the delivery is never made.

The best defense against these cyber threats is awareness. CERT-MU advises users to take the following precautionary measures during this festive season to be more secure online:

1. **Check your devices**

- Before making any online purchases, make sure the device you use to shop is up to date.
- Ensure that you have strong passwords.
- Make use of multi-factor authentication.
- Protect your devices by keeping software up to date. These include items such as mobile phones, computers, and tablets, as well as appliances, electronics, and children's toys.
- Once you have purchased an internet-connected device, change the default password and use a different, complex password (including special characters such as $@%&).
- Check the devices' privacy and security settings to make sure you understand how your information will be used and stored.
- Enable automatic software updates where applicable to run the latest version and apply the latest patches for vulnerabilities.

2. **Only shop through Trusted Sources.**

- Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor.

- Always verify the legitimacy of the website before providing any information.

- Do not connect to unsecured public Wi-Fi, especially to do your banking or shopping.

- Do not click links or download attachments unless you are confident of where they came from. If you're unsure if an email is legitimate, type the URL of the retailer or other company into your web browser as opposed to clicking the link.

- Never provide your password or personal or financial information in response to an unsolicited email. Legitimate businesses will not email you asking for this information.

- Make sure your information is being encrypted. Many sites use Secure Sockets Layer (SSL) to encrypt information. Indications that your data will be encrypted include a URL that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted.

3. **Use Safe Methods for Purchases**

- Make sure to check your credit card and bank statements regularly.
- For any fraudulent charges, notify your bank or financial institution immediately.
- Be wary of emails requesting personal information. Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information.
- Legitimate businesses will not solicit this type of information through email. Do not provide sensitive information through email.

Report Cyber Incidents

Report a cyber cybersecurity incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS+ - http://maucors.govmu.org/**)

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication, and Innovation
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org
MAUCORS: http://maucors.govmu.org