Fraud Prevention at your Point-of-Sale Device

Although today's modern point-of-sale devices include effective security features, fraudsters may still have the resources to place a skimming device on or in the point-of-sale device with the intention of collecting sensitive payment card information. It is therefore important to have fraud prevention measures in place to protect you and your business.

Visual Inspection of Point-of-Sale Device(s)

Daily visual inspections of the point-of-sale device(s) will help detect potential signs of tampering. Below are a few key indicators to be aware of when performing the visual inspection:

- The back or underside of the point-of-sale device has markings or language that are not in English
- Damaged or altered tamper seals
- Missing manufacturer labels
- Missing screws or screws with damaged heads
- Incorrect keyboard overlays which are easily detachable
- Visible external wires
- Holes in the point-of-sale device housing
- An electronic serial number that does not match the number printed on the label at the bottom of the point-of-sale device
- A high number of mag-stripe read failures or debit card declines
- Difficulty inserting a Chip and PIN card into the card reader

What to do if your Point-of-Sale Device has been tampered with

- Try not to handle the device as evidence may be damaged
- Take pictures of the device and its location in the store
- Initiate incident response procedures with RBC and local law enforcement

- Retain any video surveillance or CCTV footage that may be used to identify possible perpetrators
- Review your security procedures to identify any gaps that might have allowed the skimming incident to occur and make the required changes

Software Security Best Practices

In addition to the physical security of the point-of-sale device(s), it is important to ensure your software is also safeguarded.

- If your point-of-sale device(s) has a connection to a network via Ethernet, ensure you have a working and updated network firewall where the connection enters your location
- ALWAYS change the default admin password and ensure to update the password on a regular basis
- ALWAYS ensure the operating system is updated to the latest version

Know and Educate your Employees

You and your employees are the first line of defense against fraud. Implement strict hiring procedures to thoroughly screen potential candidates as fraudsters may attempt to join your organization. Fraudsters may also approach your employees to assist them with illegal activity. Train your employees to recognize the signs of possible fraud and skimming practices, and provide them with periodic reminders to stay alert to potential threats.

Be aware of who you grant access to the Point-of-Sale Device(s)

- Request to see ID from RBC Technical Support Staff that visit your organization if their staff ID is not visible
- Remember an RBC technician will never pay you a visit without your prior knowledge
- When in doubt, contact RBC for confirmation

Additional Fraud Prevention Measures

While there are no guaranteed measures to prevent fraud, merchants can reduce their risk by:

- Restricting the point-of-sale device(s) access to authorized employees only and never leave them unattended
- Look out for suspicious behaviour of persons or group as they might be purposely trying to distract you and your employees while their associates tamper with your device
- Safeguard point-of-sale device(s) / keypads in accordance with the merchant agreement
- Exercise due diligence to report any tampering or missing point-of-sale device(s) / keypads to RBC
- Performing visual inspections using guidelines mentioned in this brochure for signs of tampering (weekly in high-traffic areas and more frequently in locations with low foot-traffic or PIN Pad use)
- Track and report operational difficulties that occur on a regular basis.

Reminder

If you observe any suspicious activity or the point-of-sale device appears altered immediately refrain from using the point-of-sale device and disconnect it from the network connection but do not power it down. Immediately contact RBC, your security team, and/or the local law enforcement authorities, and explain your concern.

To sign up for RBC Merchant Services today, contact our team at +297 588-0101 or visit your nearest RBC Royal Bank branch.

Disclaimer

 (03/2022)