## EMV Liability Shift

**EMV is an abbreviation for Europay, Mastercard, and Visa.** These three organizations developed a new set of specifications for chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features not possible with traditional magnetic stripe cards. These new cards will retain the magnetic stripe on the back of the card for use in older POS terminals that have not migrated to the new EMV standards.

As of October 2015, if someone uses a fraudulent payment card at your business, and your POS terminal is not capable of processing chip-enabled cards, your business may be liable for the fraud charges.

Businesses should reach out to their acquiring bank or POS administrator for more information on how to obtain an EMV-compliant POS terminal.

(EMV-Connection Website)

**The Retail Cyber Intelligence Sharing Center (R-CISC) serves as the cyber security resource for the retail industry. For more information on protecting your POS system visit their website at https://r-cisc.org.**

R-CISC
RETAIL CYBER INTELLIGENCE SHARING CENTER

**If you suspect your POS system has been compromised, contact the nearest local Secret Service Field Office or please visit the U.S. Secret Service website at http://www.secretservice.gov for more details and a complete list of resources.**



*U.S. Department of Homeland Security*

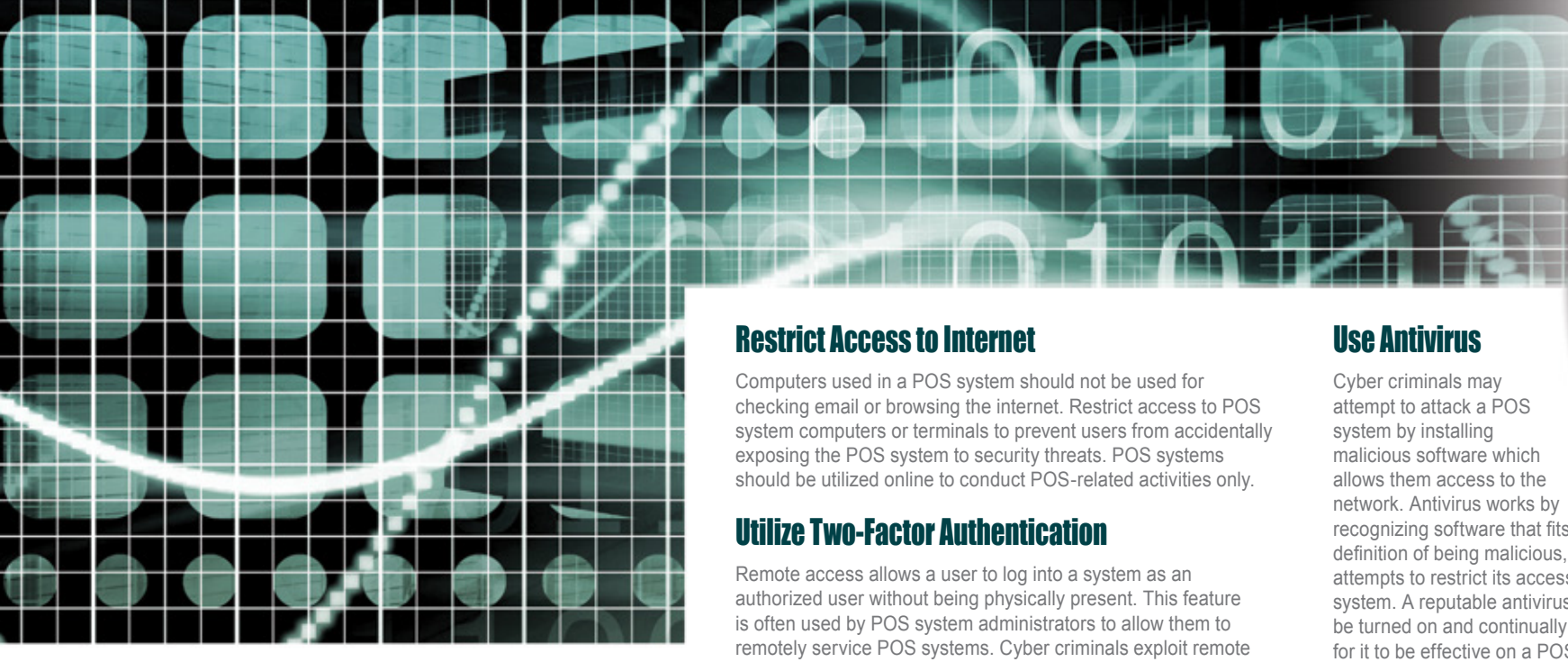
**United States Secret Service**

# Securing Sales In Retail

*Safeguarding Your Point-Of-Sale System*

*U.S. Department of Homeland Security*

**United States Secret Service**



## Point-Of-Sale

Point-Of-Sale (POS) is a term used for all applicable retail, store, checkout, or cashier systems that process the electronic transfer of payments (i.e., credit cards/debit cards, mobile payments) for goods or services.

POS hardware includes cash registers, credit card swiping devices, contactless payment readers and chip card readers that interface with an online computer system to process credit card payment information.

It is recommended that businesses work with their POS service provider in implementing the following safe practices for POS systems:

## Use Strong Passwords

Many business owners mistakenly rely on their POS system vendor to provide the necessary security for their systems. For simplicity, many POS system installers utilize the default passwords on POS systems which can be easily obtained online by cyber criminals. Business owners should change the default password, and continue to change passwords to their POS system on a regular basis, using unique account names and complex passwords.

## Restrict Access to Internet

Computers used in a POS system should not be used for checking email or browsing the internet. Restrict access to POS system computers or terminals to prevent users from accidentally exposing the POS system to security threats. POS systems should be utilized online to conduct POS-related activities only.

## Utilize Two-Factor Authentication

Remote access allows a user to log into a system as an authorized user without being physically present. This feature is often used by POS system administrators to allow them to remotely service POS systems. Cyber criminals exploit remote access configurations on POS systems to gain access to these networks. Utilize two-factor authentication, such as a password and SMS text code or a password and a security token, to ensure remote access is granted only to trusted sources with your permission.

Additionally, require POS service vendors to use two-factor authentication for remote access when possible. If two-factor authentication is not available to these vendors, disable remote access except when your business specifically schedules a service call with the vendor. Beware of social engineering calls from unknown individuals purporting to be a service technican from your vendor needing remote access to your system.

## Install a Firewall

To protect a POS system from outside attacks, a firewall should be installed and functioning. A firewall is software or a hardware device that prevents unauthorized access to or from a private network. It screens-out traffic from hackers, viruses, worms, or other malware, specifically designed to compromise a POS system. Firewalls provide security to POS systems that may be operating in an unsecure environment (i.e. the internet). It acts as the “first line of defense” against hackers or those wishing to compromise the security of your POS system.

## Use Antivirus

Cyber criminals may attempt to attack a POS system by installing malicious software which allows them access to the network. Antivirus works by recognizing software that fits its definition of being malicious, and attempts to restrict its access to a system. A reputable antivirus must be turned on and continually updated for it to be effective on a POS network. It must also be configured to quarantine and/or delete any detected file.

## Update POS Software Applications

Ensure that POS software applications are using the latest updated software applications. This is similar to a computer running antivirus software. A computer is vulnerable to malware attacks when required updates are not downloaded and installed on a timely basis. Similarly, if one does not update (patch) POS software applications, it leaves the system vulnerable to criminals who seek to exploit known software design flaws.

## Access Control

Inform employees to be on the lookout for skimmers, USB sticks, or other devices connected to the POS system. Skimmers can be installed within a few seconds while employees are distracted. Check all devices on a daily basis. Ensure that there are no active USB ports or other media drives open on a POS terminal. If running the Windows Operating System, ensure that auto-run is disabled by your service vendor. Look carefully at any transactions where the EMV chip can’t be read. Causing chip transactions to fail is a tactic used by some cyber criminals to bypass strong transaction security features afforded by chip-based payment cards.