



*die cut for business card!*

**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) for goods or services.

The POS hardware may include cash registers, receipt printers, touch-screen displays, barcode scanners, scales, and credit card swiping devices that interface with an online computer system to process credit card payment information.

This design is extremely efficient for both the retailer and the customer, but can quickly become a liability, if the following safe practices are not followed:

## Use Strong Passwords

Many business owners mistakenly rely on the POS system vendor handling the installation 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 must change passwords to their POS system on a regular basis, using unique account names and complex passwords.

## 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.

## Install a firewall

To protect a POS system from outside attacks, a firewall should be installed. A firewall is a software or 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. Antivirus must be updated continually for it to be effective on a POS network.

## Restrict Access to Internet

Computers used in a POS system must not be used for general surfing on 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.

## Disallow Remote Access

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 installers to allow them to remotely service POS systems. Cyber Criminals exploit remote access configurations on POS systems to gain access to these networks. Disallow remote access to the POS network at all times.

