Reduce remote access vulnerability with these quick tips

Many merchants rely on remote access for critical POS operations such as allowing resellers and other vendors to manage and update software systems. If not configured and managed correctly, they can provide an easy entry point for unauthorized intruders to gain access to the POS system, and potentially to sensitive customer data. The following are highly recommended tips for enabling remote access and maintaining data security.

1. Limit the number of people that can access the system remotely. Only allow and provide remote access to those who have a strong business need. This typically includes the POS system vendor/ reseller for remote service and may also include owners, management and administrators of the merchant location.

2. Use complex passwords and two factor authentications for all access in the payment environment including POS accounts and remote access. Properly store authentication/security tokens and change passwords every 90 days.

3. Do not share remote access credentials. Ensure that each user with remote access has a unique username and password. In multi-location business environments, be sure to create unique credentials for each business location.

4. Disable remote access user accounts when no longer needed.

5. Install and keep anti-virus, anti-spyware and firewalls up-to-date. Regularly run and review results of scans for malicious software.

6. Maintain up-to-date software, operating systems and web browsers at all times. Use the latest version of a remote management product or service.

7. Avoid leaving remote access software on and "listening" for incoming connections. Select a remote access package that requires a user at the merchant site to start or log on to initiate a remote access session when possible.

8. Reboot POS systems daily to clear volatile memory, and consider using a secure file wiping utility that can securely clear the contents of the page (swap) file.

9. Contact your remote access provider for additional security features they can offer and confirm their current solution provides two factor authentication to support PCI DSS requirements.

vantiv / integrated payments

smarter
faster
easier
payments™

MPD007 03.16