Secure Remote Access

WHAT’S THE RISK?

Insecure remote access is one of the leading causes of data breaches for businesses.

#1 point of entry for attacks against brick-and-mortar merchants is insecure remote access

(Point of Sale Technology Best Practices)

Point-of-sale (POS) vendors will often support or troubleshoot merchant payment systems from their office and not from the business location. They do this using the Internet and what’s called “remote access” software products. Many of these products are always on or always available - meaning the vendor can access your systems remotely all the time.

Many of these vendors use commonly-known passwords for remote access, making it all too easy for hackers to access your systems too. They scan the Internet for businesses with vulnerable remote access systems and once inside, use malware to steal valuable payment card data.

REMOTE ACCESS BEST PRACTICES

To minimize the risk of being breached, it’s important that you take a part in managing how and when your vendors can access your systems. Only allow remote access when necessary!

Limit use of remote access
Ask your vendors how to enable remote access for when they specifically request it, and how to disable it when not needed.

Require use of multi-factor authentication
If you must allow remote access, ask your vendors to use multi-factor authentication to support your business.

Require unique credentials
If you must allow remote access, make sure your vendors use remote access credentials that are unique to your business and that are not the same ones used for other customers.

RESOURCES

Visit pcissc.org/Merchants for more resources

The PCI SSC Questions to Ask Your Vendors resource can help businesses get the information you need from your third party vendors.

The PCI Qualified Integrators and Resellers (QIR) list is a resource businesses can use to find payment system installers that have been trained by the PCI Security Standards Council on secure remote access and other payment data security essentials.

The Guide to Safe Payments provides businesses with security basics to protect against payment data theft.

Watch this quick animated video to learn how businesses can minimize the chances of being breached by only allowing remote access when necessary, and using multi-factor authentication.