3 Payment Data Security Essentials SMBs Shouldn't Ignore

Attacks on POS systems at U.S. brick-and-mortar businesses are on the rise, leading to costly payment data breaches. Here are three essential data security practices SMBs should adopt now to minimize the risk of being breached:

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

Limit remote access by third party vendors. Businesses should talk to their vendors to make sure remote access to their systems is only turned on when needed, and that multi-factor authentication is being used.

** Remote Access Technology Best Practices*

80% **of hacking attacks could be prevented by strengthening passwords and installing software patches***

Install software updates or "patches". Vendors regularly issue patches to fix software vulnerabilities. Businesses should apply these security patches to their systems as soon as they receive them.

** 2017 Verizon Data Breach Investigations Report*

81% **of hacking-related breaches leveraged either stolen and/or weak passwords***

Use strong passwords and change default ones. Computer equipment and software out of the box (including POS terminals) often come with default passwords such as "password" or "admin". Businesses should change them to something hard to guess, update them regularly and never share them.

** 2017 Verizon Data Breach Investigations Report*

For more information, download Payment Protection Resources for Small Merchants at:
PCISSC.org/SmallMerchant

PCI Security Standards Council®