Protecting Your Customer’s Payment Card Data from Malware

Recent headlines announcing organizations falling victim to payment card breaches are alarming for business owners. The Payment Card Industry Security Standards Council (PCI SSC) shares steps to take to ensure your organization has the proper security controls in place to prevent a breach caused by malware.

What businesses are at risk?

- SMBs to Fortune 100 companies: hackers don’t discriminate
- No organization is immune from attack

What information is at risk?

Names, mailing addresses, credit/debit card numbers, expiry dates, phone numbers and e-mail addresses.

Once a hacker finds a vulnerability, malware is installed and can travel to networked systems installed and can travel.

Electronic cash registers and similar point-of-sale systems are targets.

Malware can disguise itself using well-known and trusted names.

Once malware is installed, criminals can do any one of the following:

- Sell the information on a black market
- Create clone cards for use in brick and mortar stores
- Use the information for online purchases
- Access via 3rd party vendors with weak security controls
- Unencrypted data
- Intrusion into 3rd party servers to mine credit card details
- Credit card numbers and e-mail addresses.
- Malware can disguise itself using well-known and trusted names

Malware can disguise itself using well-known and trusted names.

Effect on businesses:

- Loss of sales
- Damage to brand image
- Loss of sales
- Damage to consumer confidence

Effect on customers:

- Fraudulent charges
- Inconvenience
- Damage to credit score

Organizations need to develop a layered approach to security.

Here’s what you can do right now:

- Use the latest anti-virus software and keep patches up to date
- Review system logs manually or use an automatic tool to check for suspicious activity
- Update all default and staff passwords with secure passwords
- Consider implementing a:
  - PCI-approved point of interaction (POI) device with SRED functionality
  - PCI-approved point-to-point encryption (P2PE) solution
- Confirm that all third party vendors are properly implementing and maintaining security controls outlined in the PCI Data Security Standard (PCI DSS)

Vigilance is critical. Businesses must shift their perception of security from:

A MOMENT IN TIME SNAPSHOT TO BUSINESS AS USUAL

Don’t Delay, Take Action Against Malware Today!

www.pcisecuritystandards.org | PCI SSC