Point-of-Sale and E-Commerce Cybersecurity for Small Merchants

Webinar will begin promptly at 2pm Eastern
*All speakers will remain muted until that time

www.staysafeonline.org  @staysafeonline
NATIONAL CYBERSECURITY ALLIANCE

www.staysafeonline.org

@staysafeonline
Thanks to our National Sponsors

Signature Sponsor

Contributing Sponsor

Strategic Partner

CyberSecure™
MY BUSINESS
PLAN. PROTECT. RESPOND.

Over 6,000 webinar attendees

Over 5,000 workshop attendees

Over 15,000 subscribers

This was an excellent webinar with good information for small businesses and tech support companies like us who provide advice on support and security to our customers. The information covered can be passed along to our customers so they are CyberAware!
Point-of-Sale and E-Commerce Cybersecurity for Small Merchants

Lauren Holloway
Director of Data Security Standards
PCI Security Standards Council
PCI Security Standards Council

We Help Secure Payment Data

- Global, cross-industry effort to increase payment security
- Industry-driven, flexible and effective standards and programs
- Helping businesses detect, mitigate and prevent criminal attacks and breaches
PCI Security Standards and Programs

Standards, Training and Certification Programs, Educational Resources

Payment Equipment
Payment Software
Merchant & Payment Service Provider Environments

Certification – Equipment, Service Providers, Assessors, Investigators

Training – Assessors, Investigators
Organized Crime is a Business

The global impact of huge cyber security events such as the WannaCry ransomware epidemic has taken the threat from cybercrime to another level. Banks and other major businesses are now targeted on a scale not seen before.

- Europol
POS Attacks Lead to Breaches

“At 40%, payment card data is the #1 type of data targeted in a breach.”

2018 Trustwave Global Security Report

“The chances of being struck by lightning this year are 1 in 960,000. When it comes to experiencing a data breach, the odds are as high as 1 in 4.”

2017 Ponemon Cost of Data Breach Study
90% “of all accommodation breaches were POS breaches.”

2018 Verizon Data Breach Investigations Report (DBIR)
Emerging Threat: Online Skimming

- Infects e-commerce website with malicious code
- Payment card information is “skimmed” during a transaction
- PCI SSC and Retail & Hospitality ISAC issued joint bulletin to address threat
Online Skimming: How it works

- Exploiting Vulnerable Plugins
- Brute Force Login Attempts
- Phishing
- Other Social Engineering Techniques
Online Skimming:

Who’s Vulnerable

• Any e-commerce implementation that does not have effective security controls in place
Online Skimming:

Detection Best Practices

• Tools that test web applications for vulnerabilities (Requirement 6)
• File-integrity monitoring or change-detection software (Requirement 11)
• Internal and external network vulnerability scans (Requirement 11)
• Penetration testing to identify security weaknesses (Requirement 11)
Online Skimming: Prevention Best Practices

• Use malware protection and keep it current (Requirement 5)
• Apply security patches for all software as soon as notified by the vendor (Requirement 6)
• Restrict access to only what is absolutely needed (Requirement 7)
• Use strong authentication for all access to system components (Requirement 8)
• Use trusted third parties (Requirement 12)
Leading Causes of Data Breaches

- Weak and default passwords
- Unpatched software
- Insecure Remote Access
Leading Causes of Data Breaches

- Weak and default passwords
- Unpatched software
- Insecure remote access

81% of hacking-related breaches succeeded through stolen passwords, default or weak passwords.

Verizon Data Breach Investigation Report (DBIR)
Of the majority of hacking attacks could be prevented by strengthening passwords and installing patches.

Verizon Data Breach Investigation Report (DBIR)

PCISSC.org/Merchants
Insecure remote access is the number one point of entry for attacks against brick-and-mortar merchants.

Remote Access Technology Best Practices
GUIDE TO SAFE PAYMENTS

Simple guidance for understanding the risk to small business, security basics to protect against payment data theft, and where to go for help.

COMMON PAYMENT SYSTEMS

Real-life visuals to help identify what type of payment system a small business uses, the kinds of risks associated with their system, and actions they can take to protect it.
How do you protect your business?

The good news is, you can start protecting your business today with these security basics:

1. **Use strong passwords and change default ones**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

2. **Protect your card data and only store what you need**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

3. **Inspect payment terminals for tampering**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

4. **Use trusted business partners and know how to contact them**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

5. **Install patches from your vendors**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

6. **Protect in-house access to your card data**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

7. **Don’t give hackers easy access to your systems**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

8. **Use anti-virus software**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

9. **Scan for vulnerabilities and fix issues**
   - Cost: 
   - Ease: 
   - Risk Mitigation: 

10. **Use secure payment terminals and solutions**
    - Cost: 
    - Ease: 
    - Risk Mitigation: 

11. **Protect your business from the Internet**
    - Cost: 
    - Ease: 
    - Risk Mitigation: 

12. **For the best protection, make your data useless to criminals**
    - Cost: 
    - Ease: 
    - Risk Mitigation: 

These security basics are organized from easiest and least costly to implement to those that are more complex and costly to implement. The amount of risk reduction that each provides to small merchants is also indicated in the “Risk Mitigation” column.
POS Security: What Can Merchants Do?

• Regularly check payment terminals for signs of tampering
• Create list of all payment terminals along with pictures
• Frequently compare terminal to the pictures:
  • Does anything look different?
  • Are there broken seals or new seals covering screws or plates?
  • Is there different cabling?
• Never let anyone touch or replace a payment terminal without first confirming that it is authorized and legitimate
QUESTIONS TO ASK YOUR VENDORS

A list of the common vendors small business rely on and specific questions to ask them to make sure they are protecting customer payment data.

GLOSSARY OF PAYMENT AND INFORMATION SECURITY TERMS

Simplified glossary, based on PCI DSS Glossary and with extra definitions specific to small merchants.
Questions to Ask Your Vendors

PCISSC.org/merchant

Explains different types of payment vendors:

- What they do
- Which PCI SSC Security Standard or Program applies
- What a merchant can expect
Questions to Ask Your Vendors
PCISSC.org/merchant

Sample questions:

• How secure is your solution or product?
• Do you provide ongoing support and maintenance?
• What happens if there is a breach?
PCI SSC Secure Vendor Listings

**Approved PTS Devices**
PCI approved PTS Devices provide the strongest protection for payment data and enable merchants to take advantage of EMV chip, mobile and contactless technologies.

**PCI P2PE Solutions**
Point-to-Point Encryption (P2PE) technology makes data unreadable so it has no value to criminals even if stolen in a breach. In addition to encrypting data, PCI P2PE Solutions can simplify merchant efforts to comply with PCI DSS.

**Validated Payment Applications**
PCI Validated Payment Applications are payment software products that have been validated as meeting the Payment Application Data Security Standard (PA-DSS) for protecting payment data.
Trusted Partners
Qualified Integrators & Resellers (QIR)

**WHO**
Qualified Integrators and Resellers (QIRs) are vendors that are specially trained by the Payment Card Industry Security Standards Council (PCI SSC) to install software on payment systems in a secure manner.

**WHAT**
QIRs help reduce merchant risk by implementing critical security controls to mitigate the three most common causes of payment data breaches.

**HOW**
QIRs address critical controls to mitigate the three most common causes of merchant payment data breaches: insecure remote access, weak password practices, and outdated and unpatched software.

Merchants can find the list of Qualified Integrators and Resellers by visiting [PCISSC.org/QIR](http://PCISSC.org/QIR)
Payment Data Security Essentials

Awareness

PCISSC.org/merchant
Become a PCI SSC Participating Organization

PO.PCISSC.org

Benefits and Opportunities

- Impact
- Connection
- Visibility
Get Involved Today!
participation@pcisecuritystandards.org