Five Steps to Protect Your Merchants from Online Threats

By Nathan Sweaney, Security Advisor, RSPA

Greetings, RSPA members! RSPA recently brought me on board as a resource for members who have questions about information security—and my services are free! I met many of you in Las Vegas at RetailNOW 2017, and I look forward to interacting with many more of you soon.

How can I help you? Don't let your questions keep you up at night. If those issues spark fierce debate among your team, and you can't resolve them, I'm your guy!

To get you started thinking, here are just a few issues you might want to consult me about:

- Are we providing everything our customers need to be secure?
- Is this QIR program worth the cost and effort?
- How do I ensure that our remote access to support our customers is secure?
- Can I provide secure Wi-Fi on the same network as the POS system?

In *Connect*, starting in 2018, we're going to address some of the most common security questions that resellers ask. Each of five successive issues will contain an article that dives deeply into one of these questions. Here's a quick summary:

1. Secure Remote Access
Insecure remote access is, by far, the most common cause of card breaches. Properly securing remote access is crucial to both resellers and merchants; but smaller merchants will always lean on, and trust, the reseller to take care of it. We'll outline steps you should take to ensure security.

2. Password Management
Maintaining strong password practices is a foundational part of keeping systems secure. This includes the passwords used to install and support customers as well as the passwords they use to run their system. I'll walk through common mistakes, practical tips, and things you need to do.

3. Firewall Configuration
The router/firewall is the gateway to the POS network. It decides what gets in, what goes out, and who can access the network. Resellers must understand the capabilities of the devices they sell, the needs of the merchant's network, and best practices for configuring and maintaining these devices.

4. QIR Program
PCI's Qualified Integrators and Resellers (QIR) program was created to educate resellers on security best practices. I know that RSPA members have many questions about it. For instance: What's mandated? What's not? Who needs to be a part of this program? We'll look at the purpose of the program, how it applies to resellers, and some advantages of getting certified.

5. Security Testing
Security controls and practices work only if they're done without fail. Testing and validating those controls are the best ways to ensure that systems are not only installed securely, but also continue to stay that way. Most merchants don't know anything about security and rely on their trusted partners to handle it. We'll identify some ways you can provide value to your customers by helping them to stay secure.

This is far from a complete list of security concerns, but these five areas are crucial for protecting your merchants from online threats.

So, don't wait to contact me! Just shoot me an email at securityadvisor@gorspa.org—or give me a call at 704.940.4273. I'd love to help! **c**