AURORA PAYMENTS | CHOSEN PAYMENTS an AURORA company

Connected Devices Present Network Vulnerability

Technology has evolved to a point that we are now able to use voice commands to control lighting, room temperature, security systems and even sprinklers. The devices that control these things are known as IoT devices. *The **I**nternet **o**f **T**hings* includes Ring cameras, Nest thermostats and the like. Things can be controlled with your voice or the click of button on smartphone. These connected devices create vulnerability threats to your wi-fi network.

The PCI Compliance Connection

We recently shared education with you about the importance of PCI Compliance. In this blog, we will continue to share the importance your network plays in safeguarding stored credit card data. One of the primary requirements for becoming PCI Compliant is a Network Vulnerability and Penetration test. These tests check to see if hackers can access your data, penetrate firewalls or other security systems intended to prevent outside intrusion.

What Could Go Wrong?

While smart technology and devices make our lives easier at home and work, the same smart technology and devices have faced issues with data breach incidents and security hacks. We need to remember that hackers can also take control of our connected devices at any time. According to Mark Pribish, an expert in identity theft and data breach risk management, “One of the biggest concerns of IoT is managing the risks associated with a growing number of IoT devices.” Pribish is with Vero Products, an identity theft, and data breach solutions company. In addition, IoT vulnerabilities have been discovered and exposed across many industries. These vulnerabilities threaten sensitive data as well as personal safety and remain a prime target for hackers. Any organization that uses these devices needs to be prepared.

The Threat of Connectivity

When we think of connected devices, we likely think of programmable thermostats, security systems such as doorbells with surveillance cameras and microphones, Smart and Self-Driving Automobiles to name a few. In each instance, these connected devices help save money, increase efficiencies, and improve our quality of life. However, their convenience comes at a price to customer data and privacy. The same IoT devices can also give hackers and insider threats an opportunity to steal personally identifiable information leading to a consumer becoming a victim of identity theft.

Think about this: If you can unlock the front door of your house remotely, so can a hacker. If you can start your car or unlock the door locks of your car remotely, a hacker can too. And, if any of your devices or service providers are connected to the cloud to collect, store and/or transfer information, hackers and rogue employees can collect, store and/or transfer the same information.

Keeping Your Connected Business Safe

While consumers are excited to have a more connected lifestyle, you and your customers should be concerned about the increased risk of identity theft and data breach incidents. Here are a few tips for protecting your business and your customer data in several ways:

- Always change default usernames and passwords of IoT devices
- Implement strong password management, replacing passwords with pass phrases, and/or using a password manager
- Updating your antivirus security software regularly
- Check devices default privacy and security settings
- Disable remote access to IoT devices (when practical)

Every IoT device comes with a built-in Web interface to configure the settings mentioned above. In addition to securing any new smart devices you may purchase, be sure to configure any existing IoT devices. Proper configuration is mission critical, so if you are not sure how to complete these steps, be sure to reach out to an expert for assistance.

Maintaining a safe network is a responsibility all merchants have. You must keep your customers credit card data and other personal information private. Aurora Payments can help you maintain a PCI Compliant network. Call us at 833-AURORA2 (833-287-6722) or send an email to: Hello@aurorapayments.com

Connected Devices Present Network Vulnerability

Technology has evolved to a point that we are now able to use voice commands to control lighting, room temperature, security systems and even sprinklers. These devices are known as IoT devices. *The **I**nternet **o**f **T**hings* includes Ring cameras, Nest thermostats and the like. Things can be controlled with your voice or with a smartphone. These connected devices create vulnerability threats to your wi-fi network.

The PCI Compliance Connection

- Your network plays an important role in safeguarding stored credit card data
- A primary requirement for being PCI Compliant is a Network Vulnerability and Penetration test
- Tests check to see if hackers can access your data or penetrate firewalls

What Could Go Wrong?

- Smart technology and devices invite data breach incidents and security hacks
- Hackers can take control of connected devices at any time
- IoT vulnerabilities have been discovered and exposed across many industries
- Vulnerabilities threaten sensitive data as well as personal safety
- Credit card data remains a prime target for hackers
- Any organization that uses these devices needs to be prepared.

The Threat of Connectivity

- Connected devices help save money, increase efficiencies, and improve our quality of life
- Convenience comes at a price to customer data and privacy
- IoT devices give hackers and insider threats an opportunity to steal personal information
- Devices and/or service providers connected to the cloud collect, store and/or transfer information
- Hackers and rogue employees can collect, store and/or transfer the same information.

Think about this: If you can unlock the front door of your house remotely, so can a hacker. If you can start your car or unlock your car remotely, a hacker can too.

Keeping Your Connected Business Safe

Here are a few tips for protecting your business and your customer data:

- Always change default usernames and passwords of IoT devices
- Implement strong password management, replacing passwords with pass phrases, and/or using a password manager
- Updating your antivirus security software regularly
- Check devices default privacy and security settings
- Disable remote access to IoT devices (when practical)

Maintaining a safe network is a responsibility all merchants have. You must keep your customers credit card data and other personal information private. Aurora Payments can help you maintain a PCI Compliant network. Call us at 833-AURORA2 (833-287-6722) or send an email to: Hello@aurorapayments.com