Wi-Fi and Credit Card Data: A Risk You Can and Must Mitigate

August 2020

Table of Content

Wi-Fi and Credit Card Data: A Risk You Can and Must Mitigate

Who enforces data security for credit cards?

If you do business with credit cards, you need to keep credit card data safe.

Anyone can tell you that- but there are official rules with which you must comply.

Meet the Payment Card Industry (PCI) Security Standards Council. The Council has created a set of best practices known as the PCI Data Security Standard, or PCI DSS[1].

If your business processes, stores, or transmits data for payment cards of any kind from Visa, MasterCard, Discover, JCB, or American Express, you must comply with PCI DSS requirements[2].

What is the PCI DSS?

The PCI DSS describes itself as "a minimum set of requirements for protecting account data, "[3] but this belies the rigor and complexity of the PCI DSS twelve requirements.

These requirements mandate secure hardware, secure network connectivity, secure administrative protocol, and much more (Visit this page for a short overview of the twelve requirements).

The specific form of the PCI DSS inspection depends on how many transactions you process per year[4]. Very small businesses will likely be able to complete a self-audit, while larger firms will need to have an official inspection by a third-party auditor.

1 https://www.pcisecuritystandards.org/pci_security/
2 http://www.summitdata.com/Documents/WLAN_Client_Security_and_PCI_DSS_200901.pdf
3 https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
4 https://www.itgovernance.eu/blog/en/a-guide-to-the-4-pci-dss-compliance-levels

My firm has passed the PCI DSS before. Why should I worry about it again?

Small businesses may suddenly find themselves held to more rigorous PCI DSS standards when their online business grows - only to realize their infrastructures do not meet more rigorous standards.

Large businesses are already familiar with rigorous PCI DSS audits, but vigilance is still necessary. If major restructuring occurs, large businesses must ensure their infrastructure can still meet the most rigorous PCI DSS requirements.

How does Wi-Fi figure into this?

One of the most vulnerable aspects of any organization is its Wi-Fi connection.[5]

Eavesdroppers want to intercept sensitive data as it travels from one endpoint to another. On a wired connection, this is difficult for an outsider to do. On a wireless network, it's much easier.

42Gears has extensive experience helping companies comply with PCI DSS standards. We've taken the time to summarize what we think is important, and what you can do to get started complying with PCI DSS standards.

What happens to unsafe Wi-Fi networks?

There are some common ways in which unsafe Wi-Fi networks end up getting compromised:

1. **Eavesdroppers intercept your data:** If you don't scramble or encrypt the packets of data that travel in a network, eavesdroppers can "sniff" and view those packets.[2] Thieves don't have to be right beside a target to eavesdrop on Wi-Fi data. With the use of directional antennas, "sniffing" is possible from hundreds of feet away.
2. **Rogue access points confuse and compromise your devices:** Attackers can set up wireless access points close to your network. If your devices connect to that access point, the device user is at the mercy of the attacker, who can monitor everything the user does once connected.[6]

5 https://www.networkworld.com/article/3224539/5-ways-to-secure-wi-fi-networks.html
6 Gohel, P. (2017). Cyber Attacks: Are we really secure?

3. **Denial of Service overwhelms your network:** Technically, a denial-of-service attack is any attack that makes it impossible to use a network. Most of the time, this refers to an attacker quickly sending an excessive amount of information to a network, which makes the network inaccessible for legitimate users.[7,8]
4. **Misconfigured access points create chaos:** If you manage network access points without a central system to control them, inconsistencies between access points can create an entryway for attackers. This can be as simple as giving one access point a more complex password than another one.[7,9]

What security protocols do I need to select?

You will need to secure both the wired (i.e. servers) and wireless (i.e. Wi-Fi network) components of your data.

As you likely know, encryption reconfigures data so it looks like nonsense to an observer[10]. To decode this altered data, you need a cipher (or key)- which you only give to people in your network.

There are several kinds of protocols that you will need to use for comprehensive network protection.

- Wireless Security (WPA3): As the name suggests, Wi-Fi encryption protects data transmitted within a Wi-Fi network. The kind of encryption relies on the hardware (the router and receiver) you use for your Wi-Fi network.
    - The most up-to-date and widely-used form of Wi-Fi encryption is **Wi-Fi Protected Access 3,** more commonly known as **WPA3**.[11] (Note that with proper implementation, businesses can still use **WPA2** encryption and remain in compliance with PCI DSS standards)

7 https://www.us-cert.gov/ncas/tips/ST04-015
8 https://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-Security-Threats.htm
9 https://www.tutorialspoint.com/wireless_security/wireless_security_misconfigured_access_point_attack.htm
10 https://digitalguardian.com/blog/what-data-encryption
11 https://www.wired.com/story/wpa3-wi-fi-security-passwords-easy-connect/

- Wired Security (Transport Layer Security): In order to protect data relayed between your network and other networks (such as to verify credit card information), you will need to implement server protection separately from Wi-Fi protection.
    - The most up-to-date and widely-used form of inter-network encryption is **Transport Layer Security 1.3,**[12] more commonly known as **TLS 1.3** (TLS 1.2 remains in use as well[13]).

Let's look further into keeping your Wi-Fi network safe. (For more information about TLS protocol, you can visit this page.)

So does configuring the right protocols solve everything?

No.

Encryption is necessary, but there are still issues that encryption can't solve.

For example, unless you can ensure that every user cares about security, devices can still connect to rogue access points. All of the network protections you've put in place are meaningless if business devices connect to the wrong network.

How do I keep my network safe beyond encryption?

Here are a few important ways that you can protect your network (and all of the devices you have connected to the network).

1. **Name your network to blend into the background**[14] - If your network name clearly indicates the network's purpose or location (for instance, *Grocery Store Wi-Fi* or *Grocery Staff Breakroom)* it becomes much easier for malicious actors to decide which networks to attack. Using a generic network name may result in some confusion for employees and customers, but could save your company from becoming the victim of a major attack.
2. **Make sure your Wi-Fi coverage matches what you need** - You should analyze your workplace to determine how much overlap there is between the network coverage you

12 https://www.cloudflare.com/learning-resources/tls-1-3/
13 https://www.42gears.com/blog/why-its-time-to-enable-tls-1-2/
14 https://www.networkworld.com/article/3224539/5-ways-to-secure-wi-fi-networks.html

need and the network coverage you have. If your network includes coverage for areas outside of your workplace, you may need to restructure your Wi-Fi network accordingly.

3. **Change factory defaults immediately on every device**[15] - It is shocking how often employees do not change default passwords and other default device configurations. In order to keep devices secure, you must ensure that all network hardware, and all devices connecting to the network, have complex non-default passwords in place.
4. **Maintain a rigorous inventory of all devices -** If devices go missing, yet they are already configured with Wi-Fi credentials, other network security features cannot help. Keeping track of all devices at all times is important for preventing device loss. You may do this using a unified endpoint management (UEM) system.
5. **Ensure you can send emergency messages to every device** - In the event you face a major network threat, you cannot afford to keep processing credit card data until the threat is removed. If you have an emergency message system in place, you can inform anyone operating a point-of-sale device about new threats.
6. **Educate employees** - You need to teach employees about responsible network usage by conducting regular security awareness sessions. It is in every employee's interest to keep your network safe, and therefore, it is everyone's responsibility to connect to only approved networks, change passwords, and more.

How can I do these things without getting in the way of our day-to-day operations?

There's no perfect answer, but there *are* fast, non-disruptive ways to gain more control and be more vigilant.

One of them is to integrate a *Unified Endpoint Management (UEM)* system with your devices and hardware. UEM software lets admins view and manage many aspects of their network from a single central console.

Using UEM software, for example, admins can require business devices to change default passwords and require new passwords to be complex. UEM software also makes device tracking

15 https://www.infosec.gov.hk/en/best-practices/business/deploying-of-corporate-wireless-network

easy, and if something goes wrong, the central UEM console can send emergency messages to every connected device.

UEM software can also mandate devices to connect only to specific secure networks, safeguarding against any threat posed by rogue access points.

But wait- would UEM software violate PCI DSS standards?

As long as you choose secure UEM software (like SureMDM by 42Gears), you will *not* break PCI DSS compliance. This means you can use UEM software to make PCI DSS compliance easier.

In fact, the PCI Council has supported the use of a UEM solution to monitor and contain potential threats in conjunction with anti-malware software.

How can I start putting UEM software in place?

The first step towards implementing a UEM solution is creating a proof of concept - establishing that your organization can implement the technology on a small scale. 42Gears provides tools to help you with the proof of concept phase- and, when ready, the transition from proof-of-concept to full implementation.

As the first part of its commitment to a painless proof-of-concept process, 42Gears offers a risk-free 30-day trial of its UEM software. To get started, visit this link, or reach out to 42Gears using at sales@42gears.com or +1-(424)-284-2574