A Complete Guide To Wireless (Wi-Fi) Security

In the modern world, it seems as though it would be nearly impossible to function without access to the wireless internet. People everywhere rely on Wi-Fi for everything from entertainment to achieving their goals. But with the ubiquity of the internet comes an underlying danger in the form of hackers who look to exploit security flaws to gain access to your private data and information.

As we continue into a future in which everything from our phones to our refrigerators operates using a wireless internet connection, it is becoming increasingly important to understand how to keep our **Wi-Fi safe and secure**.

In this article, we will provide you with everything you need to understand the basics of **Wi-Fi security** and which wireless devices you should use in the long run.

What is Wireless Security?

Wireless security is, in essence, preventing unwanted users from accessing a particular Wi-Fi network. More so, wireless security, also known as Wi-Fi security, aims to ensure that your data remains only accessible to users you authorize.

How Does Wireless Security Work?

Wireless Security Protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the authentication security protocols created by the Wireless Alliance used to ensure wireless security. There are four wireless security protocols currently available.

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA 2)
- Wi-Fi Protected Access 3 (WPA 3)

To be sure your network is secure, you must first identify which network yours falls under.

What Are The Types Of Wireless Security?

As previously mentioned, there are four main types of wireless security protocols. Each of these varies in utility and strength.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the first security protocol ever implemented. Designed in 1997, it has become obsolete but is still used in modern times with older network devices.

WEP uses a data encryption scheme that is based on a combination of user- and system-generated key values. However, it is widely known that WEP is the least secure network type as hackers have developed tactics of reverse-engineering and cracking the encryption system.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) was developed to deal with the flaws that were found with the WEP protocol. WPA offers features such as the Temporal Key Integrity Protocol (TKIP), a dynamic 128-bit key that is harder to break into than WEP's static, unchanging key.

It also introduced the Message Integrity Check, which scanned for any altered packets sent by hackers, the Temporal Key Integrity Protocol (TKIP), and the pre-shared key (PSK), among others, for encryption.

Wi-Fi Protected Access 2 (WPA2)

In 2004, WPA2 brought significant changes and more features to the wireless security gambit. WPA2 replaced TKIP with the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is a far superior encryption tool.

WPA2 has been the industry standard since its inception; on March 13, 2006, the Wi-Fi Alliance stated that all future network devices with the Wi-Fi trademark had to use WPA2.

WPA2-PSK

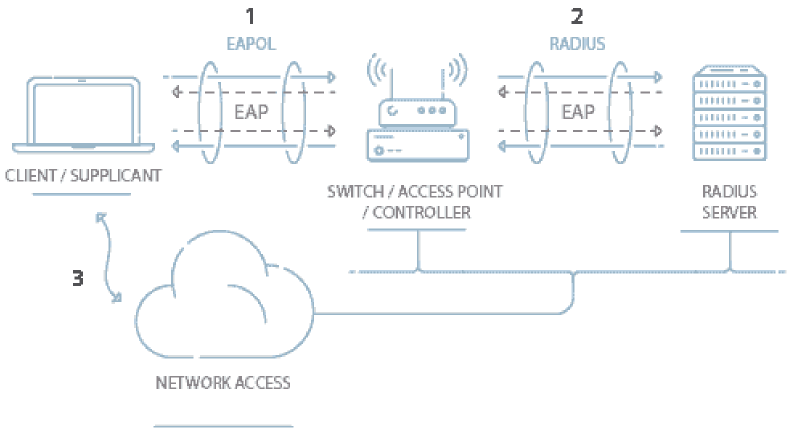
WPA2-PSK (Pre-Shared Key) requires a single password to get on the wireless network. It's generally accepted that a single password to access secure Wi-Fi is safe, but only as much as you trust those using it. A major vulnerability comes from the potential damage done when login credentials get placed in the wrong hands. That is why this protocol is most often used for a residential or open Wi-Fi network.

To encrypt a network with WPA2-PSK, you provide your router not with an encryption key but rather with a plain-English passphrase between 8 and 63 characters long. Using CCMP, that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed. Although WEP also supports passphrases, it does so only as a way to create static keys more easily, which are usually composed of the hex characters 0-9 and A-F.

WPA2-Enterprise

WPA2-Enterprise requires a RADIUS server, which handles the task of authenticating network user's access. The actual authentication process is based on the 802.1X policy and comes in several different systems labeled EAP.

There are just a few components that are needed to make WPA2-Enterprise work. Realistically, if you already have access points and some spare server space, you possess all the hardware needed to make it happen.



Because each device is authenticated before it connects, a personal, encrypted tunnel is effectively created between the device and the network. The security benefits of a properly configured WPA2-Enterprise grant a near-impenetrable network. This protocol is most often used by businesses and governments due to its heightened security measures.

SecureW2 is an industry leader in WPA2-Enterprise security solutions – everything from certificate-based authentication to device onboarding. **See how we can strengthen your network security today.**

Wi-Fi Protected Access 3 (WPA3)

WP3 is introducing the first major changes to wireless security in 14 years. Some notable additions to the security protocol are:

- Greater protection for passwords.
- Individualized encryption for personal and open networks.
- More security for enterprise networks.

WPA3-PSK

To improve the effectiveness of PSK, updates to WPA3-PSK offer greater protection by improving the authentication process.

A strategy to do this uses Simultaneous Authentication of Equals (SAE) to make brute-force dictionary attacks far more difficult for a hacker. This protocol requires interaction from the user on each authentication attempt, causing a significant slowdown for those attempting to brute-force through the authentication process.

WPA3-Enterprise

WPA3-Enterprise offers some added benefits but overall little changes in terms of security with the jump from WPA2-Enterprise.

A significant improvement that WPA3-Enterprise offers is a requirement for server certificate validation to be configured to confirm the identity of the server to which the device is connecting. However, due to the lack of major improvements, it's not likely to be a quick transition to WPA3. WPA2 became a standard in 2004, and even today, organizations have a difficult time supporting it on their network. That's why we came up with a solution that provides **everything you need for 802.1x.**

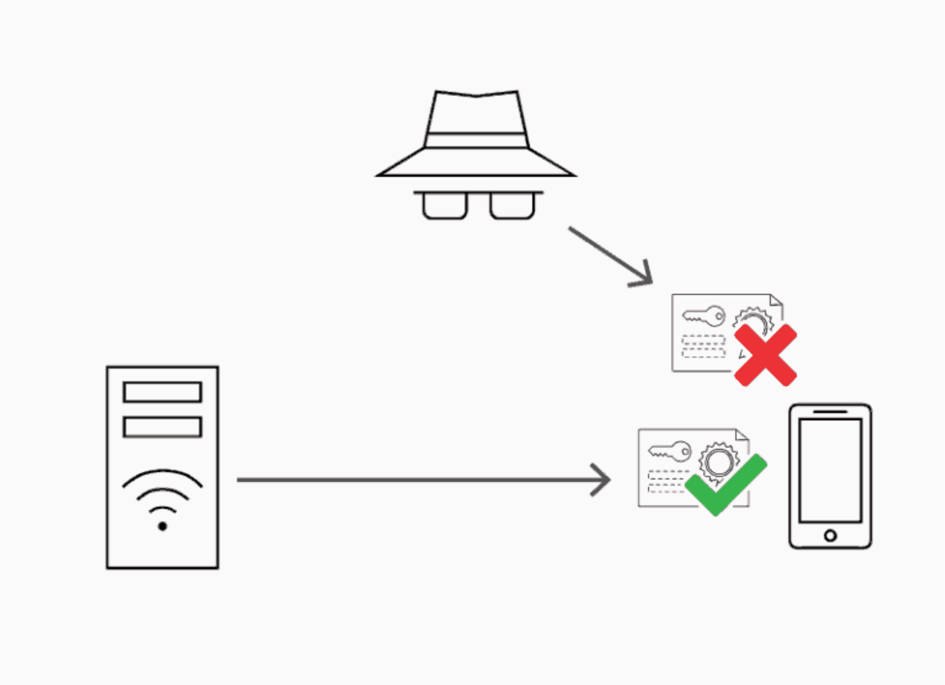
What are the Main Threats to Wi-Fi Security?

As the internet is becoming more accessible via mobile devices and gadgets, data security is becoming a top concern for the public, as it should be. Data breaches and security malfunctions can cost individuals and businesses thousands of dollars.

It is essential to know the threats that are most prevalent in order to be able to implement the proper security measures.

Man-in-the-Middle Attacks

A man-in-the-middle (MITM) attack is an incredibly dangerous cyber attack involving a hacker infiltrating unsecured wireless networks by impersonating a rogue access point and acquiring login credentials.



The attacker sets up hardware pretending to be a trusted network, namely Wi-Fi, in order to trick unsuspecting victims into connecting to it and sending over their credentials. MITM attacks can happen anywhere, as wi-fi-enabled devices connect to the network with the strongest signal and will connect to any SSID name they remember.

If you are interested in learning more about MITM attacks, read another one of our articles **here**.

Cracking and Decrypting Passwords

Cracking and decrypting passwords is an old method that consists of what is known as "A brute force attack." This attack consists of using a trial and error approach and hoping to eventually guess correctly. However, there are many tools that hackers can use to expedite the process.

Luckily, you can use these same tools to test your network's security. Software like **John the Ripper**, **Nessus**, and **Hydra** are an excellent place to start.

Packet Sniffers

Packet sniffers are computer programs that can monitor web traffic on a wireless network. They can also intercept some data packages and provide a user with their contents. They can be used to gather data about traffic harmlessly, but in the wrong hands, they can introduce errors and break down a local network.

How Do I Make My Home Wi-Fi Secure?

For your wireless network at home, it is essential that you choose the network security type that is most useful. For home wireless, it is recommended that WPA2-PSK be implemented as WPA2-Enterprise is really only needed for organizations or universities with a lot of network traffic.

Other things to consider are for your home Wi-Fi:

- Changing the default password and SSID
  - Ensure your password is at least 10 characters long and contains non-alphanumeric characters.
- Enable the router's firewall.
- Enable MAC address filtering to secure wireless access points.
- Disable remote administration.

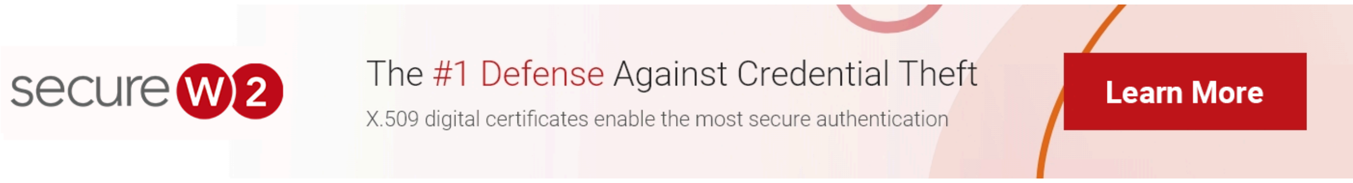
Managing Wi-Fi with Digital Certificates

Wireless networks face many security issues stemming from a common source: passwords. Passwords introduce the human error element to your Wi-Fi networks. Passwords can be stolen, lost, or even hacked through MITM or brute force attacks.

Luckily, there is an alternative through the use of certificate-based authentication. Passwords rely on keywords or phrases created by the end-user. Certificates utilize public-private key encryption to encrypt information sent over the air and are authenticated with EAP-TLS, the most secure authentication protocol.

While the costs of maintaining and implementing a PKI infrastructure to allow for certificate authentication may seem daunting, SecureW2 can offer an easy configuration to allow you to maintain the most secure internet connections easily.

How Do I Protect My Business Wi-Fi Network



WPA2-Enterprise has been around since 2004 and is still considered the gold standard for wireless network security for organizations and universities, delivering over-the-air encryption and high security. In conjunction with the effective authentication method known as 802.1X, users have been successfully authorized for secure network access for many years.

However, when using WPA2-Enterprise in a large-scale setting, it can often be challenging to configure and onboard new users.

Onboarding software, such as those offered by SecureW2, eliminates the confusion for users by prompting them with simple steps designed to be completed by anyone, regardless of technical skills. SecureW2 has the tools to make your WPA2-Enterprise network as safe as possible. **Check out our onboarding solutions here**.

LEARN ABOUT THIS AUTHOR

Eytan Raphaely

Eytan Raphaely is a digital marketing professional with a true passion for writing things that he thinks are really funny, that other people think are mildly funny. Eytan is a graduate of University of Washington where he studied digital marketing. Eytan has diverse writing experience, including studios and marketing consulting companies, digital comedy media companies, and more.

W2

TECHNOLOGY SOLUTIONS

PKI & Certificate Services

RADIUS AAA

Wi-Fi, ZTNA and VPN Security

Security for Azure

Security for Okta

VERTICAL SOLUTIONS

For Enterprise

For SMB

For Higher Education

For K12

For Service Providers

PRODUCTS

RESOURCES

JoinNow Connector PKI

JoinNow MultiOS

JoinNow Cloud RADIUS

JoinNow NetAuth

Documentation

WPA2 and 802.1x Simplified

PKI Explained

PEAP-MSCHAPv2 Vulnerability

Pitfalls of EAP-TTLS-PAP

CONTACT US

North America Sales
+1 888 363-3824
+1 512 900-5515

UK, Europe and Middle East Sales
+44 20 3912 9916

ISO 27001 Certified

SOC2 Compliant

SUPPORT

Submit a Support Ticket

Log In

Careers

PARTNERS

Okta Verified

WIRELESS BROADBAND ALLIANCE