Securing Your Firm While Working from Home

7 Home WiFi Security Recommendations

BY NICK SIVOVOL,
INNOVATIVE COMPUTING SYSTEMS, INC.

Your Firm & Remote Work: Securing Home WiFi Networks

With the dynamic consumer technology landscape, legal technology experts may never be able to secure legal professionals' home networks and personal devices to the same degree they can office-based technology. Nonetheless, law firm technology managers must extend information security practices beyond their traditional office and courtroom walls. Ensuring remote workers implement a few basic security precautions when working outside the office is one of the easiest — if often overlooked and not practiced — methods of enhancing a firm's cybersecurity.

Contact Innovative Computing Systems

Get more tips to improve your firm's cybersecurity and learn about Innovative Computing Systems, Inc.

1-800-541-0450
sales@innovativecomp.com
www.innovativecomp.com

30+ Years Of Excellence
Innovative Computing Systems
Trusted Legal Technology Partner

Below are seven tips to help you secure your home network from unauthorized access.

1. **Change the default name of your home Wi-Fi network**

   One of the first steps towards safer home Wi-Fi network is to change the SSID network name. This name is broadcast publicly and makes it easier for a hacker to identify his target. Often times these are set to a company name, a last name or a device manufacturer. The best practice is to change the network's SSID to something that does not disclose any personal information.

2. **Change your default wireless network password and make it unique and strong**

   Majority of routers come pre-set with a default password. This password is easy to guess by hackers, especially if they know the router manufacturer. A good password for your wireless network consists of at least 20 characters and includes upper and lowercase letters, numbers, and various symbols. This change will make it difficult for unauthorized users to access your network.

3. **Enable network encryption**

   All modern wireless routers come with an encryption feature. This feature is not always on by default. Turning on your wireless router's encryption setting will secure your network. Encryption should be turned on during wireless network installation. At the very minimum encryption should be set to WPA2 and if available should be set to WPA3.

4. **Disable WiFi network name broadcasting.**

   It is highly recommended that you disable wireless network name (SSID) broadcasting to the public. This feature is often useful for businesses, libraries, hotels and restaurants that want to offer wireless Internet access to customers, but it is usually unnecessary for a private wireless network.

5. **Apply WiFi router software updates.**

   Manufacturers constantly update software for their devices in order to keep them more secure and stable. A router's firmware, like any other software, contains flaws that can become major vulnerabilities unless they are fixed by firmware releases. Always install the latest software available on the system and download the latest security patches to ensure no security hole or breach is left for hackers to exploit. Most routers now come with an auto-update option that should be turned on.

6. **Turn on your WiFi router's built-in firewall.**

   A "firewall" is designed to protect computers from harmful intrusions. Wireless routers generally contain built-in firewalls and other security features but are sometimes shipped with them off. Be sure to check that the wireless router's firewall and security features are turned on. If a firewall or security features are not available, then you should look into upgrading your router/firewall with a better solution such as Fortinet FortiGate.

7. **Create a Guest wireless network.**

   Most Wi-Fi routers now come with an option to setup a guest wireless network which is isolated from the regular network and all devices. This is a great option when giving Internet access to your guests or friends as it will keep the rest of your network secure. Guest network should be secured with a strong password and follow the above-mentioned procedures and best practices.

Over 30 years of legal technology experience.

Innovative Computing Systems, Inc., has primarily focused on the technology needs of law firms since 1989, and those skill sets have been sought out by entities such as municipalities, corporate environments and professional services organizations. Innovative Computing Systems takes a best-of-breed approach to all its offerings. Innovative Computing Systems selects only premier technology partners to provide solutions to its clients and is committed to maintaining long-term strategic relationships with them to ensure the highest levels of success, both in productivity and with IT initiatives proper. Learn more by visiting www.innovativecomp.com.

www.innovativecomp.com

1-800-541-0450

Los Angeles | San Francisco | Austin