GPSOLO
SOLO, SMALL FIRM & GENERAL PRACTICE DIVISION A PUBLICATION OF THE AMERICAN BAR ASSOCIATION

Network Cybersecurity in Your Home and Office

Vol. 35 No. 2

By John Bandler

John Bandler is founder of Bandler Law Firm PLLC, which helps firms, businesses, and individuals with cybersecurity, cybercrime investigations, litigation support, and other areas. Previously, he was a state trooper, then a prosecutor who investigated global cybercrime. Now he is the author of the book Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security *(ABA, 2017). For more information, please visit cybersecurityhomeandoffice.com.*

A short while ago we all became network administrators without realizing it and without much training. Before that, we owned a single computer that connected to the Internet with a telephone line, and data flowed between the computer and the Internet through that cord. Eventually we got broadband Internet, and then the number of our computer devices began to multiply and they all needed Internet access, and physical connections were inconvenient. WiFi networking was born, soon became commonplace, and now is a necessity. It allows multitudes of devices to share Internet access, along with other resources such as printers and stored data.

About GPSolo magazine

GPSolo magazine is published six times a year (January/February, March/April, May/June, July/August, September/October, and November/December) by the ABA Solo, Small Firm, and General Practice Division.

GPSolo is devoted to themes of critical importance to your practice. Each issue contains articles exploring a particular topic of interest to solos, small firms, and general practitioners, as well as articles related to technology and practice management. And to keep you up to date, each issue contains five *Best of ABA Sections* digests, reprinting the top articles published by other ABA entities that will be of the greatest interest to you.

Many purchased a WiFi router and were more concerned with getting it to "work" than with making it secure. We set it up quickly, connected our devices to it, they were magically able to access the Internet, and then we forgot about it. Security was less than an afterthought—it was a neverthought—and many were unaware of the privacy and security risks.

The potential harm was evident to me when I was a junior prosecutor trying to identify a cybercriminal who—among other things—exploited this risk. He used the Internet to traffic in stolen credit card numbers, transact in virtual currency, and conduct fraud. One technique to remain anonymous was to "borrow" the Internet access of his neighbors through their unsecured WiFi networks, which were available for him to join without a password. When I tried to trace his location, it came back to a variety of neighbors, and in three distinct neighborhoods. It was only when other leads revealed a suspect, and I learned his address and where his mother and girlfriend lived, that his use of neighbor WiFi became apparent. This is just one of many ways that poorly secured WiFi can be exploited; cybercriminals also can access poorly secured WiFi networks in a business and steal business data.

Today's WiFi routers are shipped with better default security, but the default is not perfect, and our understanding of the networks we create and administer is sometimes lacking. An important ingredient for protecting our security and privacy is knowledge, a fundamental premise of my book, *Cybersecurity for the Home and Office.* We all understand how and why to lock the front door of our home or office, now it's time to understand how to lock our electronic doors and restrict who can access our network and computers. The "Internet of Things" (IoT) and connected (or "smart") homes mean that many people connect devices to their network without sufficient consideration. You don't need to become a professional network administrator, but merely improve your knowledge and understanding a little bit. (For an overview of cybersecurity basics, consider reading my September/October 2017 *GPSolo* article, "Cybercrime and Fraud Prevention for Your Home, Office, and Clients.")

How Networks Work

Networking is the process of moving data and getting it to where it needs to go. Think about a combination mailroom and security desk that reviews incoming mail and visitors, tries to make sure they are in the right place, and routes them to where they need to go. This function is performed by each computer and then by the router for the network.

Your computer—whether it is a smartphone, tablet, laptop, or desktop—has a network interface controller (NIC) that basically performs this gatekeeper and sorting role. Thanks to the NIC and

- Visit the ABA Solo, Small Firm, and General Practice Division
- More publications from the Solo, Small Firm, and General Practice Division

Subscriptions

More Information

- Editorial Board
- Copyright Information
- Reprint Permission
- Advertise with Us
- Author Guidelines [PDF]

Contact Us

Robert M. Salkin
Staff Editor
American Bar Association
321 N. Clark St.
Chicago, IL 60654-7598
Phone: 312-988-6076
Fax: 312-988-6081

Jeffrey Allen
Editor-in-Chief

Kimberly Kocian
Director
ABA Solo, Small Firm, and General Practice Division

the software surrounding it, multiple applications can have multiple simultaneous conversations with distant locations on the Internet. Data is flowing in and out constantly and never gets mixed up. Your web browser can have multiple tabs open, each communicating with a different website, and other applications can check for new e-mail, text messages, social media updates, and more.

Now let's think about a small home network that is created by the WiFi router, which allows multiple devices to access the Internet through it. Just as one computer needs to keep track of multiple Internet conversations from its many applications, your network needs to keep track of multiple conversations coming from multiple devices, all using the shared Internet access. See Figure 1 for a simple diagram of a home network.

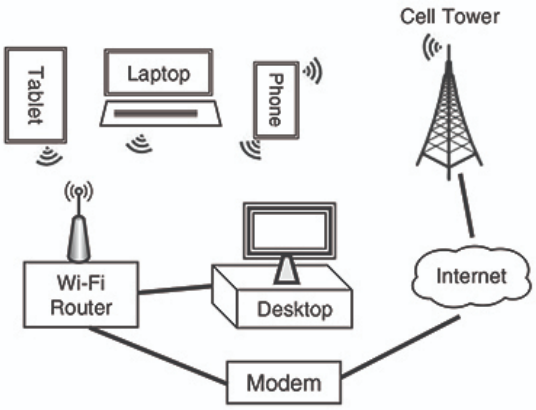

Figure 1: Sample Home Network

Note that our smartphones have two paths to the Internet: through our home WiFi and through the cell tower using the cellular provider's network. With many computers sharing a single Internet access point, the router needs to keep track of the variety of conversations each is having on the Internet. Any data going to or from the Internet must go through the router, and the router keeps track of it all. A dozen devices—smartphones, tablets, laptops, and desktops—all share the WiFi network created by the router. The router "routes" all the data to where it is supposed to go, out to the Internet or in to the correct computer.

Now let's talk about Internet protocol (IP) addresses. Basically, any computer that communicates with other computers needs an IP address, which is similar to a mailing address. Your Internet service provider (ISP) provides you with a "public" IP address, which you use to access the Internet and communicate on the Internet, and every place you communicate with via the Internet has its own public IP address, too. Your router creates a local area network (LAN) and assigns every device on the local network its own unique "private" IP address for communication within this local network. The router translates and routes data to the Internet,

allowing all devices to share the same public IP address while each retains a unique private IP address, as illustrated in Figure 2.

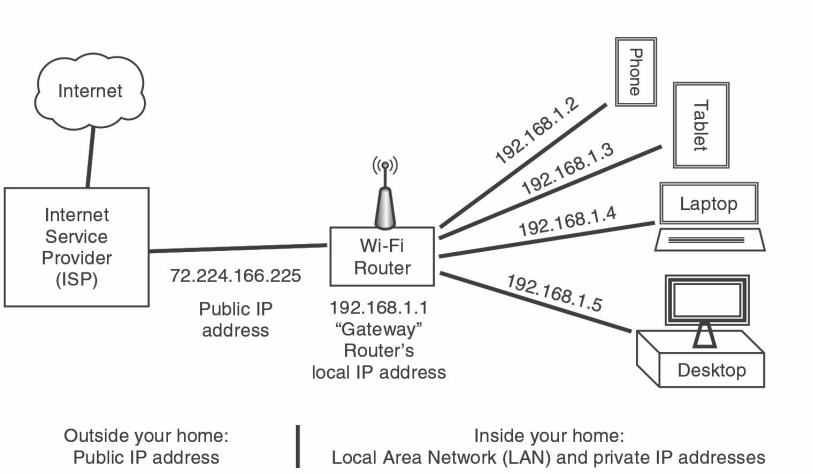

Figure 2: Network Address Translation and IP Addresses

Secure Your Network

Now that you know the basics of networking, it's easier to start improving your security. Cybersecurity always starts with physical security, so evaluate who has physical access to your router or network connections. Your home and office are probably secure, but remember that systems can be compromised by someone with physical access.

The remaining steps are improved by note taking. Blank paper works, or use the form I created for this purpose, "Form 4: Network and Internet Summary," available through cybersecurityhomeandoffice.com/book/forms. Print the form to paper, fill it out by hand, and then keep it in a place where you can find it while keeping it relatively secure.

An article in a lawyer magazine yearns for disclaimers and warnings—so here they are. Security improvements should be made incrementally and gradually, when you have the time and patience to deal with any hiccups. Move deliberately, think twice before making changes, and make notes of what you do. Alterations can affect your network and disconnect devices from it, requiring you to reconnect them.

1. Log into the router administration portal and review the login user name and password. Ensure you are connected to your local network, and use your web browser to navigate to the IP address of your router administrator portal, also known as a "default gateway." In Figure 2 it is 192.168.1.1, but yours may be different. When you figure out yours, write it down on the form.

Enter the username and password to access your router's administration portal. If it is a default username and password, such as "admin/admin," you must change it. Criminals know these default passwords and can gain access to your network. Make sure

the password is not a default, is strong, and write it down on the form.

2. Update your router firmware. Your router has an operating system, called firmware. Like any software, it isn't perfect; bugs, flaws, and security vulnerabilities are continually identified. For example, a vulnerability known as "KRACK" was recently identified that could allow a hacker to access your WiFi network. When manufacturers learned of this, they modified (patched) the firmware and put out an update for users to download. However, many users take a long time to implement patches, leaving them vulnerable to this attack and others.

After you log in to your router administration portal, check for a firmware update, install it, and note the date on the form.

3. Review router options, disable unneeded options, and enable security features. Take a tour of your router's administration interface and see what options exist. Don't be intimidated, and don't expect to learn it all at once. Some options are for security, some are for convenience, and one rule of cybersecurity is to disable features that you do not need. Every feature comes with a vulnerability.

Your router may have a convenience feature called WiFi protected setup (WPS) to allow you to connect devices to your WiFi network with the push of a button. It is a security risk, so disable it. By reading this article, you have demonstrated you don't need it and are able to keep track of your WiFi password.

Your router may have a feature to allow you to access your home computer remotely. This sounds wonderful, but consider that hackers could try to access your home computer with this tool also. If you don't need it or don't know how to secure it, disable it. Other features such as universal plug and play (UPnP) might not be needed and could be disabled. Your router has security features that are helpful to enable, such as a firewall, or blocking of malicious sites.

Review the devices connected to your network; you may be surprised at how many there are.

4. Review your WiFi network name and password. The WiFi network name (also known as SSID, or service set identifier) should be evaluated. If a hacker decided to target you for some reason, don't make it so easy to be found by naming it after you. Consider also that your computing devices may "call out" for known or trusted networks, and the WiFi name might share information you don't want to share. Simply put, the SSID name communicates information about you, wittingly or not, even when you travel. Consider the malicious use of an SSID name recently in the news, where a Turkish Airlines passenger created a WiFi network named "bomb on board," creating alarm and causing the plane to divert and land.

The WiFi network must be password protected to prevent anyone from easily joining it; anyone who joins can use your Internet connection, eavesdrop on your network communications, and potentially compromise your computing devices. The WiFi password should be strong, which means long and somewhat complex, and not something like "123456" or "wifipassword."

Write the WiFi network name (SSID) and WiFi password on the form. If you decide to change either the SSID or password, any device that previously connected to the network will be logged off and will need to be reconnected.

Review the WiFi encryption settings. The WiFi network should be encrypted and use a current and strong encryption method, such as WPA2. Standards change, and you should not use obsolete encryption such as WEP.

5. Enable the guest network. Enable your router's guest network feature if available. It allows you to provide Internet access for guests and specific devices without providing access to your entire network and other computing devices. This is in accordance with the information security principles of "least privilege" and network segmentation.

6. Disconnect when not needed. Incessant connection to the Internet can be harmful to our cybersecurity as well as our mental health. If your device doesn't need to be connected to the Internet, consider putting it in airplane mode or turning it off. We are dependent on a constant connection to the Internet, but we need to realize this connection is the path criminals will take to get to us. Criminals, through malware and bots, are constantly probing and exploring the Internet, looking for any router, device, or website with weak security. Turning your device off or disconnecting it from the Internet helps reduce the threat.

7. Avoid public WiFi. Every time you connect to a network, you are putting yourself at the mercy of others connected to the network. They can potentially eavesdrop on the data you send and receive, and compromise your computer. Consider a public WiFi network like a noisy stock market floor where shouting traders stand shoulder-to-shoulder when conducting business. Data is flowing at a rapid rate, and there is no privacy in these communications within the network. Any computer on the network can overhear what is being said to another computer, unless the data is encrypted. The lesson is to think before joining a particular network.

Instead of using public WiFi, consider using your smartphone as a hot spot. In essence, your smartphone creates a WiFi network, to which you connect your tablet or laptop for Internet access. Another way to protect yourself is by purchasing a traveling hot spot service from a cellular provider and configuring it securely.

8. Consider what data is transmitted and how. Take a moment to consider the transmission and receipt of data between your device and various destinations on the Internet. Could someone—either within your local network or somewhere along the Internet—eavesdrop on your activity? Data encryption in-transit protects against this. For example, when you use your web browser to connect to an Internet site and the site is HTTPS (rather than HTTP), you see a green padlock in the address bar, which means the data you are sending and receiving is securely encrypted in transit. This protects the confidentiality and integrity of the message.

Another way to protect your communications is through a virtual private network (VPN) service. You would use the VPN service as an Internet proxy: Your data goes from your device to the VPN, then from the VPN to the place on the Internet you are connecting to. While your data is in transit between your device and the VPN, it is encrypted, making it hard for an eavesdropper to know what data you are sending or receiving, and what Internet sites (aside from the VPN) you are communicating with. If you use a VPN, you must choose one that is reliable and trustworthy—you are putting all your communications into the hands of the VPN.

If you're interested in learning more about the applications sending or receiving data, take a look at the Windows Task Manager or Mac Activity Monitor.

Conclusion

I hope this short primer has improved your knowledge and skills, which will allow you to better secure your home and office and also give better advice to your clients about the legal risks of poor cybersecurity.