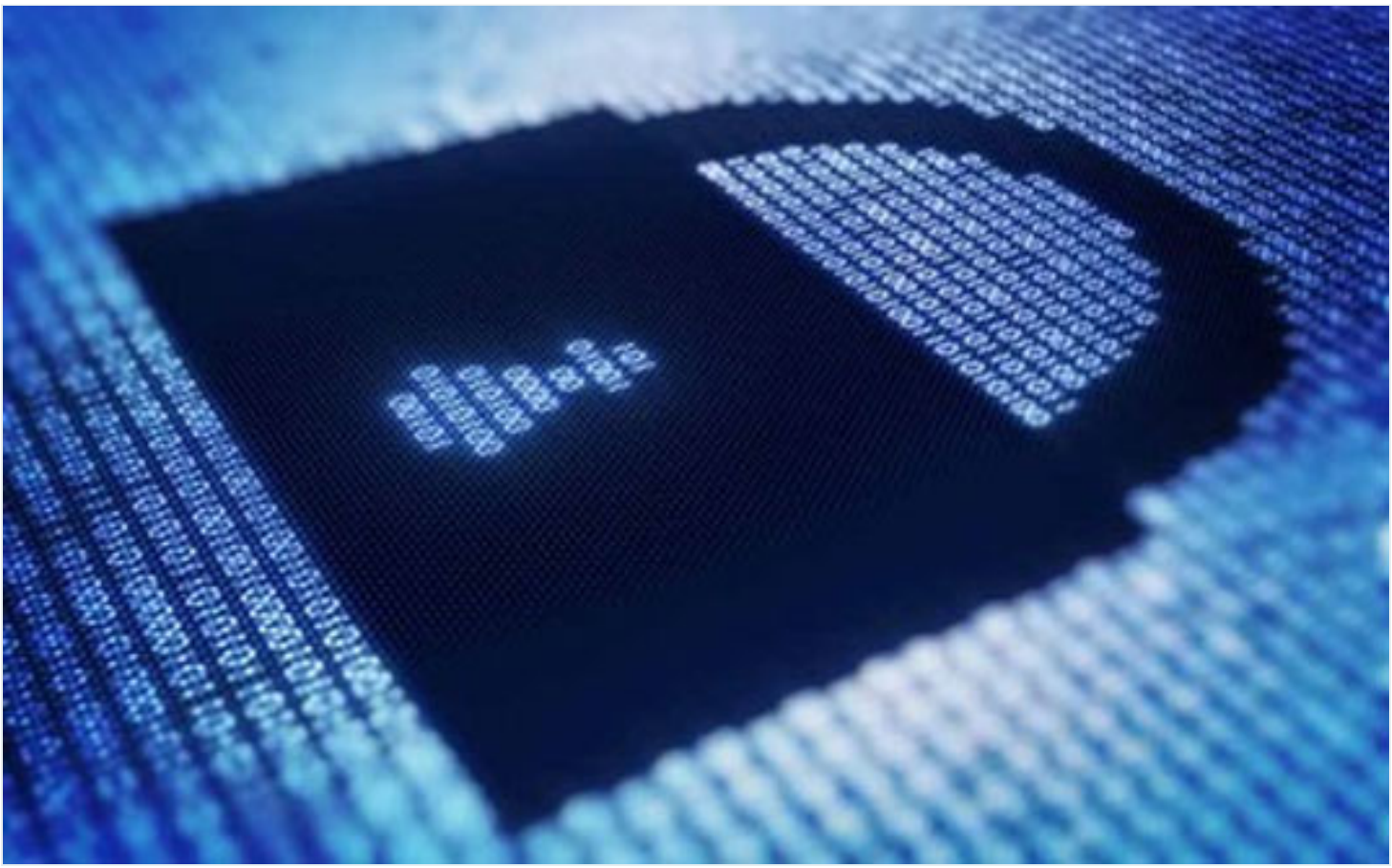
creating a Virtual Private Network (VPN) with another computer, perhaps using the internet to connect a device to a server at your office. We will discuss Wireless ...

Brian Tankersley • Nov. 13, 2022



Note: This is part three of a series of articles on basic tools used to encrypt confidential data to protect it from unauthorized access. The first column discussed practical methods to encrypt data "at rest", while the second one details encrypting data while it is "in transit" with secure portals and encrypted messages.

I was at the barber shop recently, waiting for my appointment, and another patron asked the barber, "Do you have Wi-Fi?", and the barber pointed at a sign on the wall with the name of the wireless network, which was an "open" wireless network that

had no security. While we have all used public wireless networks, whether in barber

The shocking reality is that unless you use one of these technologies, some of the data you transmit over an open wireless network can be intercepted on a nearby computer and read by someone else – think of this as "digital eavesdropping". When you connect to Wi-Fi at a coffee shop, use wireless internet on an airplane, or connect at a hotel or restaurant, you should assume that everything you do can be watched by your neighbors.

In the early days of wi-fi, many users I know had their e-mail credentials and messages stolen out of thin air over the wireless network in hotels, and over 10 years ago we adopted VPNs or use our own cellular internet connection devices instead of the unencrypted hotel internet. The standard rule became "no public Wi-Fi" use permitted, and this rule is likely to change as noted below.

Wireless Network Encryption

While no current wireless security standard is perfect, Wi-Fi Protected Access (WPA2) is one of the most secure protocol] available in current networking hardware used to encrypt data while it is being transmitted over the radios used in a wireless network. When you connect to a wireless network with WPA2, you must have the name of the network (SSID) as well as enter a shared "network security key" which is used to identify you as an authorized user of the network. The network security key also facilitates your computer and the wireless access point hardware exchanging encryption keys (strings of data used like passwords) with each other.

Your Wi-Fi radio then uses the encryption keys to scramble data it transmits over the wireless network and descramble radio signals received from the access point's radio over the wireless network. Since the encryption keys on each computer are unique to your device, and only the wireless access point can decrypt each individual conversation, you can't snoop on the radio traffic of other devices even though you're using the same network, secured with the same network security key.

A new standard called WPA3 has been approved and when implemented, it will

with virtual private networks.

Brian F. Tankersley, CPA.CITP, CGMA (@BFTCPA, CPATechBlog.com) advises firms and companies on accounting technology issues. He has served as the technology editor for a major accounting industry publication, and currently teaches courses in the US and Canada through K2 Enterprises for professional accounting organizations across the US and Canada. Brian and his family make their home in Farragut, Tennessee.

Firm Management • Hardware • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.