If you're traveling July 4th, be careful with free Wi-Fi and protect your data

July 4 2019, by Jefferson Graham, Usa Today

Credit: CC0 Public Domain

You can protect yourself during the holiday weekend if you change your passwords twice, subscribe to a VPN app, encrypt your data and avoid using public Wi-Fi in a hotel, restaurant or airport, says security expert Ted Harrington.

Okay, that seems rather extreme, but he does have a point.

Public Wi-Fi is a great way for hackers to tap into your personal information, especially during high trafficked times like a holiday weekend.

The service "may be monitored by malicious attackers, especially in airports or hotels," says Harrington, executive partner at Independent Security Evaluators.

But the fact is, you are going to use Wi-Fi over the next few days, without thinking twice about it. So how can you be safe? Let's look at Harrington's tips. Perhaps there are a few you'll sign up for.

Buy your own Wi-Fi

You can pick up a personal hot spot device (usually known as MiFi units) from a wireless provider, which will give you your own private Wi-Fi network. The bonus is that you get to access Wi-Fi from anywhere you are. The downside is that they are very pricey. Verizon's starts at $150 and demands a two-year $29.99 monthly contract. Retailers like Best Buy have several less costly options starting at around $29, plus $10-a-month service fees with companies like UnrealMobile.

A less costly option is to turn your phone into a hot spot to connect to the computer (this bypasses the public Wi-Fi). However, if you're on a limited data plan, you may not have enough data available to pull this off, or the costs of going over your limit may be prohibitive.

An alternative: Buy a pre-paid wireless card from a big box retailer, and use that service instead. Net10, for instance, offers 4 gigabytes of data for $35, as a one-time charge. The 4 GB won't last long but should be enough to check travel arrangements, e-mail and post on social media on

a week trip.

Get a VPN app

A VPN (virtual private network) "allows you to create a secure connection to another network over the internet," and shields "your browsing activity from prying eyes on public WiFi," says Harrington. Three popular VPN apps include NordVPN ($6.95 monthly for one year), SurfShark ($5.99 monthly for one year) or TunnelBear ($4.99 monthly for one year.)

Encrypt

Beef up your passcode for the phone, to ensure that your data is safe. For instance, don't be like rapper Kanye West, who displayed his iPhone passcode, 000000, during a televised meeting with President Donald Trump. Make it a little more challenging to the hacker, by skipping on your birthday, home address or other easily Googled personal info. Remember that the keys also have letters, and a 6-character code could be your favorite song or place you've visited. Say you went to San Francisco in 2018, and your code could spell out San F 18, or 726318.

Two-Factor

Apple and Google also encourage the use of two-factor authentication, which sends you a text after you log in, for the second level of security. This extra step will usually stop hackers from your case, as they move on to easier prey, says Harrington.

Change passwords

It's a pain, but important because as Harrington notes, hackers look for

simple ways to get into your account, like people who use easy to crack passwords like 123456 or their address.

To ease the pain of having to remember the constantly changing passwords, try a password manager.

"This adds another level of protection against passwords and data being stolen if a phone or device is hacked," says Harrington.

Popular managers, which create the new passwords for you and remember them, include LastPass (starts at $3 monthly) and Dashlane ($5 monthly.) Dashlane's services come with a free VPN service that "encrypts your online activity on unsecure Wi-Fi networks to always keep your personal information safe and private." However, users have to remember to open the app and turn on and off the VPN feature.

Back home

Harrington says you should change passwords again, just to be safe, especially from any website where you input personal data, like social media, work, e-mail, communication and collaboration platforms.

The odds are, you probably won't do this, so just remember—when using the free public Wi-Fi, please don't do anything sensitive like banking of financial planning, or anything that involves social security and other important numbers.