

Is Using Public WiFi Still a Bad Idea?

It depends, security experts say. Encryption has made web surfing safer but not risk-free.



April 12, 2019



iStock-496814499 iStock-979000796

Security experts have long advised people to avoid using public WiFi networks because of the risk of being hacked.

Despite those warnings, free WiFi is becoming more widespread and popular, with consumers browsing the web courtesy of local governments, cable companies, neighborhood coffee shops, and others that offer an on-the-house hot spot.

The question is: Are those fears still warranted? Most sensitive data is now sent through encrypted channels. Many of the risks with public WiFi have faded since many adults began their online lives, according to Chester Wisniewski, a principal research scientist for the British cybersecurity firm Sophos.

What's New From Consumer Reports

Get trusted advice delivered twice a week straight to your inbox.

By clicking "Sign Up" I agree to the [Privacy Policy](#) and [User Agreement](#), and consent to receive promotional emails.

Sign Up 

MORE ON SECURITY &
PRIVACY

**Who Is Watching You? CR
Helps You Take Control of
Your Digital Privacy.**

**Privacy Fix: How to Find
Old Online Accounts**

Wisniewski likens worries about digital security to evolving concerns over automotive safety. A generation ago it was difficult to persuade people to wear seat belts, but these days that battle has largely been won—and safety

How to Set Up a Smart
Speaker for Privacy

Are Health Apps Putting
Your Privacy at Risk?

5 Easy Ways to Protect
Your Digital Privacy in 2019

experts have new concerns.

“If I were lecturing kids about driving now, it would be about texting, which didn’t exist when I was learning to drive,” he says.

In the digital world, phishing emails and ransomware attacks mean that cybercriminals have much easier and more lucrative ways to make money than by lurking in a Starbucks trying to hack customers' laptops.

But not everyone agrees. Gary Davis, chief consumer security evangelist for the antivirus software maker McAfee, says that the old-school dangers remain.

“Things are much safer now that just about everything is encrypted,” he says. “But that doesn’t suggest the threat’s gone away.”

Here are the main questions to think about if you're deciding how to use public WiFi.

Will Encryption Protect You?

One of the biggest game changers in WiFi safety is the now widespread use of encryption. Transport layer security, or TLS, is used to encrypt data sent between your browser and the servers it’s trying to access. It’s signified with an “HTTPS” in a web address, as well as a little padlock logo.

TLS scrambles the data, leaving it all but useless to any attacker who might intercept it, including hackers who can carry out “man in the middle” attacks by using the

same WiFi network their target is using.

Encryption was once reserved for banking sites and others that routinely traffic personal information. But now it's standard on just about every major website, including Amazon, Google, and Wikipedia.

According to Mozilla, about 87 percent of the web traffic to U.S. users of its Firefox browser is now encrypted. That's up from about 73 percent in January of this year and 56 percent a year before that. That's the good news.

But experts warn that TLS encryption isn't perfect. It can be broken by sophisticated hackers.

“Even HTTPS can be hijacked and downgraded,” says Clay Miller, chief technology officer for SyncDog, which focuses on mobile security. “Meanwhile, a lot of files, PDFs, medical records, and bank statements still aren't encrypted.”

A recent study by researchers in Italy and Austria found that about 5.5 percent of the top 10,000 websites secured by HTTPS had TLS security flaws that could make them vulnerable to man-in-the-middle attacks or allow an attacker to at least partly decrypt them.

In addition, while you can look for the trusty padlock if you're on a laptop or desktop computer, that isn't as easy on a mobile device, especially when you're using apps that don't show web addresses at all.

For this reason, even Wisniewski agrees that when using phone apps, it's better to play it safe and rely on the phone's cellular data connection, which is generally much more secure than an unsecured WiFi hot spot.

Are Municipal Hot Spots Safer?

Many people might be wary of WiFi at their favorite neighborhood haunts but feel more comfortable jumping on a connection provided by their city or their cable company. Website encryption aside, don't those big, professionally managed networks have their own security measures in place?

Some do. But municipal and corporate WiFi networks are not all created equal, and consumers should do their homework before going online.

For example, New York City operates two WiFi networks: an open network that doesn't offer any protection, forcing you to rely on website encryption or protection built into your device, and a private network that encrypts all of the traffic that passes through it.

Both are free to the public, and all that's needed to register is an email address. The encrypted network also requires you to download a digital security key, and it currently can be accessed only from Apple mobile devices.

The city encourages anyone using the unsecured network to stick with encrypted websites and avoid any sensitive activities such as banking or credit card transactions.

The situation is similar with Optimum, a division of Altice USA that provides cable and internet services, including a large network of WiFi hot spots in the New York tri-state area. The company says that it encrypts customers' log-in information when they sign on to its

hot spots but that they're largely on their own after that while browsing the web.

Optimum encourages users to make sure their firewalls and antivirus software are up to date, and it offers a free security suite that includes those elements.

Are You Really a Target?

Like a lot of security-related decisions, deciding whether or not to use public WiFi comes down to judging the trade-off between security and convenience. It's up to you to decide whether the benefits are worth the risks.

If you're a government official with state secrets on your phone or an executive for a Fortune 500 company with plans for your next great product on your laptop, the decision to stay off public WiFi is an easy one, Wisniewski says.

But for ordinary people, most have only a certain amount of patience and effort to spend when it comes to staying safe online. Wisniewski thinks that effort would probably be better spent locking down their accounts with better passwords and two-factor authentication.

"What would be lost if you got man-in-the-middle at Starbucks?" he asks. "Will I log on to my bank account at Starbucks? No. But will I log on to Twitter? Sure."

But Davis counters that even if the odds of someone getting hacked are extremely remote, letting go of good habits is a bad idea.

"We, as security professionals, need to think about how

best we can keep consumers informed and educated,” he says. “To say they don’t need to worry about public WiFi anymore probably sends the wrong message.”

The bottom line: Public WiFi is safer now, but it's not entirely safe. That's especially true if you're using mobile apps, where there's often no way to tell whether data is being encrypted.

How Can You Stay Safe?

Here are a few tips for staying safe online, especially if you’re using a public WiFi connection.

Use strong passwords. Wisniewski says bad passwords are his No. 1 security pet peeve. Long strings of random characters are best, and don’t be tempted to use the same password for multiple accounts. Credential-stuffing attacks, where hackers use armies of bots to run lists of previously stolen passwords against other accounts, are on the rise.

Enable two-factor authentication (2FA). Requiring a second element for logging on to a website, such a passcode texted to your phone or a physical key you insert into your computer, goes a long way toward keeping hackers out even if your password is compromised.

Be careful what you post. Social media accounts can be a virtual gold mine for hackers looking to crack your passwords. Be careful about posting too many personal details.

Consider using a VPN. Virtual private networks

encrypt all the data traveling back and forth from your device. Miller says they're great protection against man-in-the-middle attacks. But not all security experts agree. Wisniewski thinks that they're unnecessary and that many are too awkward for most consumers to use.

Encrypt your devices. A VPN and TLS security protect your data in transit, but Miller says you need to make sure that what's stored on your device is secure, too. That way, if someone gains access to your device, your data will remain scrambled. With smartphones, doing this is as simple as setting up a passcode. But encrypting laptops can take a bit more work.

Beware of phishing. Emails that appear to be from your bank or credit card company could actually be from a hacker trying to gain access to your account. Clicking on a link in one of those emails could send you to a fake website designed to steal your log-in credentials or result in malware or spyware being installed on your device. You're better off just typing the URL of the financial institution directly into your browser.

Delete old information. There's no reason to keep copies of three-year-old tax returns saved on your work laptop or mobile device. Personal documents are better backed up at home. And regularly deleting documents you don't need anymore reduces what hackers can steal, Miller says.

Concerned about who's watching you? CR shares easy and effective ways to take more control of your digital privacy.

Tips for Using Public WiFi

Think all public WiFi is safe? Think again. On the "Consumer 101" TV show, Consumer Reports expert Maria Rerecich explains to host Jack Rico how hackers can use rogue networks to steal your personal information.



For 90 years, we have been fighting to make sure you get a fair deal and safe products. Our scientists, engineers, journalists, and researchers work tirelessly to bring consumers like you trusted information, so you have the answers you need. Not just so you can buy an appliance or car with confidence, but also so that you can know what's safe for you and your family. As a nonprofit organization, we rely on the support of our members to help raise the standards of the products and services we use every day. Every donation, no matter the size, contributes to this work. **Please support Consumer Reports today – even a gift of as little as \$3 will help. Thank you.**

Select a Donation Amount

\$3

\$15

Other

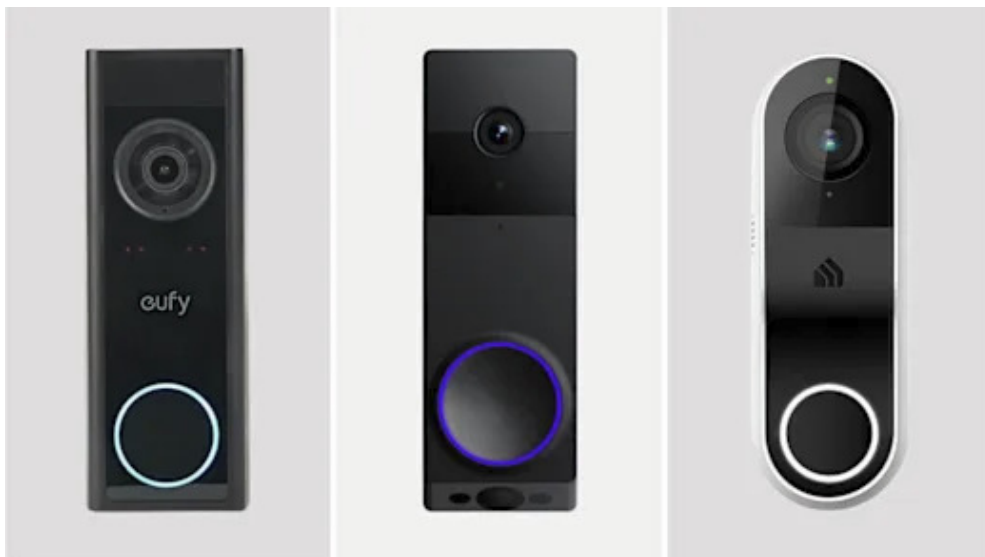


We're counting on you

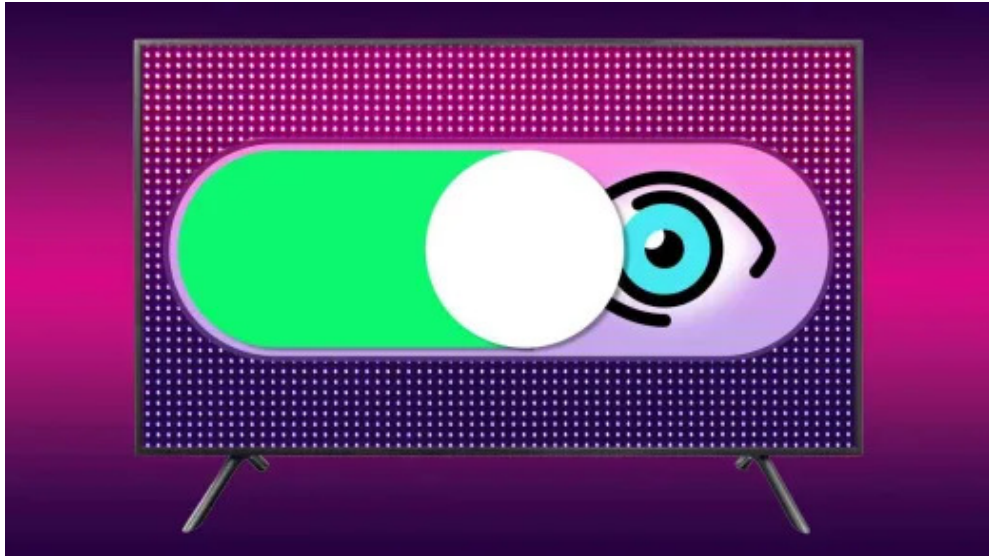
Support CR's independent testing with your \$5 donation today.

[Give Now](#)

Trending in Digital Security



10 Best Video Doorbell Cameras of 2026,
Lab-Tested and Reviewed



How to Turn Off Smart TV Snooping Features



Should You Use Passkeys Instead of Passwords?



How to Wipe a Computer Clean of Personal Data

Consumer Reports is an independent, nonprofit member organization that works side by side with consumers for truth, transparency, and fairness in the marketplace.

Become a Member

Give a Membership

Reviews & Advice

- Appliances
- Babies & Kids
- Cars
- Electronics
- Health
- Home & Garden
- Money
- All Products
- A-Z

For Businesses

- Brand
- Licensing
- Data
- Intelligence
- Innovation
- Partnerships

Company

- About Us
- Careers
- Media
- Room
- Advocacy
- How
- Donations
- Help
- Make a Donation
- Give a Membership
- Annual Meeting

Support

- Contact Us
- Account
- Settings
- About Membership
- Submit a News Tip

Resources

- CR Magazine
- CR Store
- Newsletters
- Video
- en Español
- fb.com/SomosCR

