BankOnITUSA®

INFORMATION SECURITY BRIEF

OCTOBER 2021

Free Wi-Fi Isn't Always Free

Public internet isn't secure. Here are some tips to protect your personal info when you're out and online.

The Internet is always with us. We've become so used to jumping online at any given moment — whether it's to look up directions, check work email, or post a photo — that we don't even think about it. But in virtual life, as in real life, the moment you let your guard down, you become vulnerable to bad actors who are just waiting to take advantage.

Free Wi-Fi at your local coffee shop, library, hotel, or airport is great for keeping you plugged in when you're away from your home router. But you should be aware that any unsecured network is susceptible to savvy hackers who can easily tap in and syphon off your data.

BankOnIT is dedicated to helping financial institutions build, streamline, and safeguard their information networks. In other words, banks trust us to guard their most valuable data — your personal financial info. So, we've got some tips on how to protect yourself while using free public Wi-Fi:

- **Whom Do You Trust? —** All public Wi-Fi comes with risk. Still, some networks are more trustworthy than others. First, it's best to limit the number of networks you join and to make sure those few are the real deal. Think of it as a Circle of Trust. If the business doesn't display its network name and password, ask an employee to make sure you get the right one. And try to avoid any third-party networks that may or (more likely) may not have anything to do with the shop or restaurant you're sitting in.
- **Always Read the Fine Print —** When a network's log-in page pops up to ask if you agree to terms, you should know what you're clicking into. They might be gathering data — you have a right to know what they intend to use it for.
- **Listen to Your Browser —** A lot of the more popular browsers, like Google Chrome or Safari, will warn you when a site you're trying to access isn't secure. Don't just click through.
- **Update Your Antivirus Software —** If you're surfing on a laptop, make sure you have the latest updates to look out for new malware that might be trying to sneak into your system.

BankOnITUSA®

INFORMATION SECURITY BRIEF

- **"S" Stands for Security —** Look for "https" in the web address, as opposed to just "http." This doesn't necessarily mean the site is on the level, but at least you have a secure connection.
- **Use a VPN —** A virtual private network, or VPN, encrypts your information so that even if someone is watching, all they see is a scrambled mess of characters.
- **Scroll Like Someone's Watching —** Follow your instincts. If you're using a public wireless network, don't do anything you wouldn't want a nosy stranger to see. Steer clear of websites that use your personal information, particularly your social security number, credit card numbers, or any bank account numbers. In fact, it's probably best to avoid any online money transactions on public Wi-Fi.

The only surefire way to be safe while surfing the web out in the world is to stay off public Wi-Fi altogether. For instance, your smartphone is a much safer option, either in your hand or as a portable hotspot for your computer, because mobile data is usually encrypted. But if there's no other option, remember to be cautious. You never know who might be watching.