

Traveling Safe

Value security over convenience while traveling.

As more of our transactions take place in the digital world, more of our personally identifiable information (PII) is available to others. While PII provides the ability to quickly identify individuals, it also allows bad actors to steal your identity and act on your behalf without your consent. Criminals are constantly evolving their tactics to trick unsuspecting people into exposing personal information unknowingly. When traveling our information can still be at risk. Tourists experience a higher rate of scams because they are new to that area and are targeted by bad actors. Please utilize the information below to stay secure when traveling.

Best Practices for Traveling Safe

It's important to remain vigilant while traveling and to always be aware of your surroundings. Before you take your next trip, here are some things to consider to stay protected.

Avoid using public Wi-Fi

- Typically, these networks are unsecured and should only be accessed after enabling a Virtual Private Network (VPN) or a mobile hotspot to keep yourself protected.
- Using VPN will encrypt your data and hide your IP address, making for safer internet browsing.

Be wary of public USB charging stations

- Public USB charging stations have the potential to be loaded with malware which could allow bad actors to access your sensitive information.
- Add a 'block' to your USB cord to use an outlet for charging and reduce your risk.
- Use a portable charger to charge devices.

Avoid using a debit card for payments

- If possible, avoid using debit cards for purchases while traveling and use credit cards or third-party apps (Apple Pay, PayPal, etc) because it's easier to submit fraud claims.

Protect your accounts

- Add purchase alerts to your accounts to monitor unauthorized transactions.
- If possible, add security alerts to your accounts so you'll receive notifications for any changes made to the security settings of your account.

Research the location of your travels

- Educate yourself on common scams in the area you may be traveling to.
- Stay vigilant of your surroundings and know how to contact local authorities.

Protect your devices

- Keep your devices close and secure when in public places such as hotels, restaurants, and airports.
- Be cautious of shoulder surfers who may try to steal your information by looking at your screen.

International Travel

International travel can create more opportunities for bad actors to take advantage of you and try to steal your information. Stay vigilant when traveling internationally and read about local scams in the area that you are traveling to. Please only connect to Wi-Fi that is trustworthy with strong passwords and that is not available for anyone else's use. It is recommended that you use a Virtual Private Network to connect securely.

What is a Virtual Private Network?

A VPN, or Virtual Private Network, is a service that creates a secure, encrypted connection between your device and the internet. This connection helps protect your online activities from being monitored or intercepted by others. They hide your IP address and encrypt your internet traffic, making it difficult for anyone to track your online activities which can help protect your data from hackers, especially when using public Wi-Fi networks, and help you stay anonymous online by masking your location and identity.

This material is for general information only and is not intended to provide specific advice or recommendations for any individual. This material was prepared by LPL Financial, LLC

Tracking #703378

Exp 03/2027