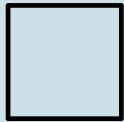


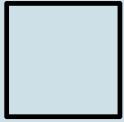


SHEPHERD
SECURITY

Travel Security Checklist



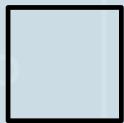
Travel lightly - Limit the number of devices you take on your trip. The more laptops, tablets and smartphones you take, the more risk you open yourself up.



Check your settings - Check the privacy and security settings on web services and apps. Set limits on how and with whom you share information. You might want to change some features, like location tracking, when you are away from home.



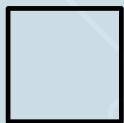
Update your software - Update your mobile software before you get on the road. Treat your mobile device like your home or work computer. Keep them updated during your travels by turn on “automatic updates” on your devices if you’re prone to forgetting. Keeping your operating system software and apps updated, will improve your device’s ability to defend against malware.



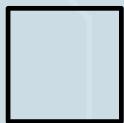
Back up files - Back up your information. Back up your contacts, photos, videos and other mobile device data with another device or cloud service. If your device is lost, stolen, broken or you otherwise lose access to it, you won’t lose all your data. You can back up your data on the cloud, on an external device like a hard drive or, preferably, both.



Set up the "find my device feature" - Set up the find my device feature on all your devices. This will help you find your phone, tablet or laptop if you lose it and might allow you to disable or wipe data from it if it gets in the wrong hands.



Password protect your devices - Set your devices to require the use of a PIN, passcode or extra security feature (like a fingerprint or facial scan). Get into the habit of locking your device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or destroy your information.



Protect your login with MFA - Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.