Digital Safety for Travelers

Protecting Your Devices, Data, and Digital Identity While Traveling

Published August 2025 | SafelyArrived.com | Updated regularly as policies change

Pre-Travel Digital Preparation

Device Security Setup

- Update all software - operating systems, apps, and security patches
- Enable strong authentication - two-factor authentication on all accounts
- Set strong passwords - unique passwords for each account
- Enable device encryption - full disk encryption on laptops and phones
- Activate find/wipe features - remote location and data erasure capability

Data Backup and Protection

- Complete data backup - all important files to secure cloud storage
- Test backup restoration - ensure backups work before traveling
- Remove unnecessary data - minimize sensitive information on devices
- Encrypt sensitive files - additional protection for confidential data
- Create offline copies - important documents accessible without internet

Account Security Review

- Review account permissions - apps and services with access to your data
- Enable login notifications - alerts for suspicious account access
- Update recovery information - ensure you can regain account access
- Pause unnecessary services - reduce digital footprint while traveling
- Inform banks of travel - prevent fraud alerts on legitimate transactions

WiFi and Internet Security

Public WiFi Safety Protocols

- Use VPN services - encrypt all internet traffic
- Verify network names - confirm legitimate WiFi networks with staff
- Avoid sensitive activities - no banking or confidential work on public WiFi
- Turn off auto-connect - prevent automatic connection to unsafe networks
- Use cellular data - mobile hotspot instead of public WiFi when possible

Hotel and Accommodation WiFi

- Ask for official network name - verify with front desk or staff
- Check network security - prefer password-protected networks
- Use hotel ethernet - wired connections are generally safer
- Monitor connected devices - disconnect unused devices
- Log out completely - clear browsing data after each session

Internet Café and Business Center Safety

Device Protection Strategies

Physical Device Security

- Never leave devices unattended - in hotels, restaurants, or transportation
- Use device locks - screen locks, cable locks, and security cases
- Keep devices visible - maintain control in crowded areas
- Distribute devices - don't carry all electronics in one bag
- Use hotel safes cautiously - for non-critical items only

Theft Prevention and Response

- Record device serial numbers - for insurance and recovery purposes
- Take photos of devices - proof of ownership for insurance claims
- Enable tracking features - Find My iPhone, Find My Device
- Test remote wipe - ensure you can erase data if device is stolen
- Have replacement plan - know how to get emergency device replacement

Airport and Transportation Security

- Keep devices charged - avoid borrowing chargers or using public charging stations
- Use charging protectors - data-blocking USB adapters
- Separate valuable electronics - during security screening
- Monitor devices during screening - watch for tampering or theft
- Secure devices during sleep - on flights and long transportation

Social Media and Communication Safety

Social Media Guidelines

- Limit location sharing - avoid real-time location posts
- Delay travel posts - share experiences after returning home
- Review privacy settings - limit who can see your posts and information
- Avoid itinerary details - don't share specific travel plans publicly
- Be cautious with photos - avoid images that reveal location or valuables

Communication App Security

- Use encrypted messaging - Signal, WhatsApp, or similar secure apps
- Verify contacts - ensure you're communicating with intended recipients
- Avoid sensitive topics - assume all communications may be monitored
- Use disappearing messages - for sensitive conversations
- Keep app versions current - install security updates promptly

Email and Work Communication

- Use secure email services - avoid unencrypted email for sensitive information
- Be cautious with attachments - don't open unexpected files
- Verify sender identity - confirm important messages through alternate methods
- Use work VPN - for accessing company resources remotely
- Follow company policies - adhere to organizational digital security guidelines

International Digital Considerations

Border and Customs Security

- Understand search rights - some countries can search devices at borders
- Minimize sensitive data - remove confidential information before travel
- Use encrypted storage - protect sensitive files with strong encryption
- Know your rights - research digital privacy laws in destination countries
- Have legal contacts - know who to call if devices are confiscated

Government Surveillance Awareness

- Research local laws - understand digital monitoring practices
- Use secure communication - encrypted apps and VPN services
- Limit sensitive activities - avoid controversial or sensitive online behavior
- Consider burner devices - temporary phones/laptops for high-risk destinations
- Document normal device state - record what's normally on your devices

Internet Censorship and Access

- Research internet restrictions - blocked websites and services
- Download content offline - maps, guides, and entertainment before arrival
- Use reliable VPN services - research which VPNs work in your destination
- Have backup communication - alternative methods if primary services are blocked
- Understand penalties - legal consequences of circumventing restrictions

Financial and Payment Security

Digital Payment Safety

- Use secure payment methods - chip cards, contactless payments, trusted apps
- Monitor accounts regularly - check transactions frequently while traveling
- Enable transaction alerts - immediate notifications of all account activity
- Use travel-friendly cards - no foreign transaction fees, chip and PIN capability
- Have backup payment methods - multiple cards from different providers

Banking App Security

- Download apps before travel - avoid downloading financial apps on foreign networks
- Use official app stores only - never download banking apps from third-party sources
- Enable app-specific PINs - additional security layer for financial apps
- Log out completely - don't stay logged in to banking apps
- Use secure networks only - avoid banking on public WiFi

Cryptocurrency and Digital Wallet Safety

- Use hardware wallets - keep cryptocurrency offline when possible
- Backup recovery phrases - store securely, separate from devices
- Research local regulations - cryptocurrency laws vary by country
- Limit mobile wallet amounts - only carry small amounts for daily use
- Monitor exchange rates - be aware of conversion fees and rates

Set up your SafelyArrived check-in at safelyarrived.com No app. No download. If you don't check in — your emergency contacts are automatically notified. Be Prepared. Not Scared.