

# Vacation Prep Checklist

## If you find that you have been affected by cybercrime during your vacation, follow these immediate action steps:

- Call your bank, credit union or credit card provider to inform them of potential fraud and close or change any compromised accounts.
- Change passwords and pins for any of your affected accounts.
- If your social media or email accounts have been compromised, notify your family, friends and coworkers.

For more incident specific help, visit [FightCybercrime.org](https://FightCybercrime.org).

## Before you go:

- **UPDATE SOFTWARE**  
Ensure that your software is current on all of the devices you plan to bring. Old software may have security vulnerabilities.
- **PASSWORD-PROTECT YOUR DEVICES**  
Be sure that your laptop, smartphones, and other electronic devices are password-protected before you travel.
- **WRAP-UP YOUR BANKING AT HOME**  
This tip goes for all internet tasks that handle sensitive information or involve downloads of any kind. It's best to finish these tasks while you're on your own WiFi.
- **NOTIFY YOUR FINANCIAL INSTITUTIONS**  
Let your financial institution and credit card provider know that you will be traveling so they can keep an eye on your accounts.

## During your stay:

- **BE WARY OF HOTEL WI-FI**  
Don't do any internet tasks that handle sensitive information or involve downloads on public Wi-Fi.
- **USE A WIRELESS HOTSPOT OR VPN**  
If you need to do internet tasks that involve sensitive information, use a wireless hotspot or VPN.
- **SECURE YOUR VALUABLES**  
Lock up any valuables, including any documents containing sensitive information, in your hotel safe when you are out of your room.
- **CHOOSE YOUR PAYMENT METHOD WISELY**  
Credit cards have more protection against fraudulent charges than a debit card.