BCD travel

CHECKLIST

HOW TO STAY CYBER SECURE WHILE TRAVELING

7 tips for business trips

Business travelers can and should take steps to secure internet-enabled devices during domestic or international trips. The proactive safety measures help make travelers less desirable to criminals and ultimately less vulnerable to cyber-attack.

1

If you connect it, protect it.

Keep device software up to date. Where possible, sign up for automatic updates and protect devices with antivirus software.

2

Back that thing up.

Back up contacts, financial data, photos, videos, and other important information to a cloud service or an external drive.

3

Double your login protection.

Enable security settings such as multi-factor authentication (MFA) to ensure that you're the only person with access to your accounts.

4

Don't auto-connect.

Disable the auto-connect feature on all devices so that you're the one actively choosing to connect to a safe network.

5

Stay protected while connected.

Before connecting to any public wireless hotspots (airports, hotels, cafes, etc.), be sure to confirm the network name and login procedures with staff to ensure network legitimacy. Don't access sensitive information on public networks. For added security, only use sites with URLs that begin with https://.

6

Play hard to get.

Don't respond to or click links and attachments in suspicious emails.

7

Don't click and tell.

Limit the information you post to social media, including seemingly innocuous information such as your favorite café or home address. These details seem harmless but are all the information criminals need to target you. Make sure your social media accounts are set to private and you're only connecting with people whose profiles you deem reasonably secure.

Travel smart. Achieve more.

Get more done with our How-to series for people who work and manage travel.

Questions? Email: move@bcdtravel.com