Summer Travel

Cybercriminals don't take summers off, leveraging relaxed attitudes toward work and personal activities to execute their scams. We outline the risks and mitigation tactics below, so you can ensure your security while out, about and abroad.

Risks	Mitigation Tactics
Public Wi-Fi networks are often unsecured, making it easy for hackers to intercept data transmitted over these networks,	Use a virtual private network (VPN) when connecting to public Wi-Fi networks to encrypt data transmission and enhance security.
Traveling increases the risk of physical theft of devices like laptops, smartphones, or tablets, putting sensitive data in the hands of potential scammers.	Enable remote tracking and wiping features on devices to locate or remotely erase data if the device is lost or stolen.
Individuals may be more susceptible to social engineering attacks, where hackers manipulate them into divulging sensitive information.	Always be skeptical about unsolicited requests for sensitive information and only give it out after verifying the identity of the requester as legitimate.
Misplacing or having devices stolen while traveling can lead to unauthorized access if the devices are not adequately protected	Implement strong passwords, biometric authentication, and encryption on devices to protect data even if the device falls into the wrong hands.
In unfamiliar environments, individuals may be more likely to download malicious software or malware disguised as legitimate applications,	Install reputable antivirus software and only download applications from official app stores or trusted sources, avoiding suspicious links or pop-ups.
When crossing international borders devices may be subject to inspection by border security agents, potentially leading to privacy concerns or data exposure.	Use encryption and password protection for sensitive files and store sensitive data in encrypted containers or cloud storage with strong security measures.
Working from public places such as cafes, airports, or co-working spaces may expose individuals to shoulder surfing or physical tampering of their devices.	Use privacy screens or work in areas with limited visibility to prevent shoulder surfing, and always lock devices when stepping away, even for a brief moment.
Using location-based services or sharing whereabouts on social media can compromise personal privacy and expose individuals to physical security risks.	Disable location-sharing features on social media platforms and adjust privacy settings to limit the visibility of location information to trusted contacts only.
Managing data backups while traveling may be more challenging, increasing the risk of sensitive data loss in the event of device theft, damage, or malware infection.	Maintain regular backups to the cloud or external drives, and consider automated backup solutions so that data is consistently protected, even while traveling.

Barracuda®
Your journey, secured.