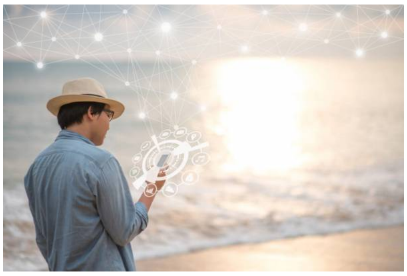
BUSINESS TRAVEL – TRAVELING IN SAFETY



The role of technology in global travel and business travel is becoming more significant. With the development of advanced technologies like 5G and blockchain, its importance is expected to increase further. These technologies have built-in protocols that make them perfect for travel applications as they facilitate data storage and access.

Data Security

Access to information at all times is crucial for the industry, as information exchange is vital between companies. For instance, travel agencies transmit customer information to hotels and airlines. Blockchain technology enables capturing all travel process information, from traveler preferences to flight and hotel prices. Hospitality companies can use this technology for baggage tracking, identification services, and customer loyalty programs. Blockchain decentralizes and organizes data, providing high security and ensuring that information is always accessible and secure from user errors or cyber-attacks.

Too traditional?

Indeed, security is crucial and should not be taken lightly. A recent survey conducted by BCD Travel on travel payments and spending revealed that 17% of business travelers had fallen victim to credit card fraud while traveling.

The TMC survey of more than 1,300 business travelers worldwide found that the vast majority (79 percent) still use a traditional corporate credit card or a personal card (26 percent), with only 1 percent of travelers saying they use virtual cards, which can automatically generate a unique virtual card number for each transaction and link all charges to a specific reservation, significantly reducing the risk of fraud.

Staying up to date

When traveling, and not just for business, experts recommend practicing safe online behavior and proactively protecting Internet-enabled devices. Whether it’s a computer, smartphone, gaming device, or other devices, the best defense against malware and viruses is updating security software, web browsers, and operating systems.

Other important aspects include:

- Backing up contacts, financial information, photos, videos, and other data from the mobile device to another device or a cloud service.
- Limiting connections to trusted people, although some social networks may seem safe.
- Enabling automatic updates by setting security software to run regular scans.

Experts also suggest enabling multi-factor authentication for email, banking, social media, and any other service requiring a login to ensure that only you can access your account.

Turning off automatic connections

When traveling, turn off automatic connections. Some devices automatically search for and connect to available wireless networks or Bluetooth devices, but these connections allow cyber criminals to access devices remotely. Turn off these features to have control over when you connect to a secure network.

Before connecting to it, verifying the security and staff availability of a public wireless hotspot, such as those found in airports, hotels, or coffee shops is essential . If the access point is unsecured, avoiding sensitive activities requiring passwords or credit card information, such as banking, booking, or company data, is best. Using a personal hotspot is often safer than relying on free Wi-Fi.

Date: 2023-07-19

Article link: https://www.tourism-review.com/business-travel-safety-tips-news13429