DIGITÁLNÍ BEZPEČNOST

BEZPEČNOSTNÍ DOPORUČENÍ

Velké mezinárodní sportovní akce pravidelně přitahují oportunistickou kriminalitu zaměřenou na mobilní zařízení, finanční účty a osobní údaje. Většině incidentů lze předejít dodržováním základních zásad kybernetické hygieny, fyzického zabezpečení zařízení a situačního povědomí.

Českým cestovatelům se doporučuje registrace v systému DROZD před odjezdem.

Oblast hrozby	**Bezpečnostní doporučení**
Příprava zařízení	• Aktualizujte telefony, notebooky, tablety a aplikace před odjezdem. • Aktivujte vícefaktorové ověřování (MFA) pro e-mail, bankovnictví a sociální sítě. • Zapněte šifrování zařízení a možnost vzdáleného vymazání dat.• Před cestou zálohujte důležité soubory.
Veřejné Wi-Fi a internet	• Pokud možno se vyhýbejte otevřeným veřejným Wi-Fi sítím. • Používejte důvěryhodnou VPN na všech veřejných sítích. • Před připojením si u personálu ověřte oficiální Wi-Fi síť stadionu nebo hotelu. • Vypněte automatické připojování k Wi-Fi a Bluetooth.
Nabíjení a USB rizika	• Pokud možno se vyhýbejte veřejným USB nabíjecím stanicím. •Používejte vlastní nabíječky nebo powerbanky. • Zvažte použití USB datových blokátorů ke snížení rizika tzv. „juice jackingu“.
Krádeže telefonů a notebooků	• Mějte zařízení pod fyzickou kontrolou v přeplněných fanouškovských zónách, na letištích, ve veřejné dopravě a na stadionech. • Nepokládejte telefony na stoly v restauracích ani je nedávejte do zadních kapes. • Používejte tašky nebo pouzdra s ochranou proti krádeži. • Ztracená nebo odcizená zařízení okamžitě uzamkněte a na dálku vymažte.
SIM karta a mobilní bezpečnost	• SIM karty nakupujte pouze od důvěryhodných poskytovatelů nebo v oficiálních kioscích. • Chraňte SIM kartu PIN kódem. • Zvažte využití důvěryhodných eSIM služeb, které omezí manipulaci s fyzickou SIM kartou. • Sledujte náhlé výpadky služby, MFA výzvy nebo neočekávané uzamčení účtů.
Finanční bezpečnost	• Pokud možno používejte bezkontaktní platby nebo bezpečné digitální peněženky. • Neprovádějte bankovní operace přes veřejné Wi-Fi sítě. • Pravidelně kontrolujte své účty kvůli podvodným aktivitám. • Zvažte používání RFID ochrany pro platební karty a pasy.

Vytvořeno: SIHASO US
Sihaso.cz / Sihaso.com

Ochrana soukromí a identity	• Zvažte vytvoření dočasné e-mailové adresy pro registrace, přístup k Wi-Fi a vstupenky. • Zvažte používání dočasného telefonního čísla nebo sekundárního čísla při sdílení kontaktních údajů. • Omezte sdílení osobních údajů s neznámými prodejci, aplikacemi nebo jednotlivci.
Sociální sítě a podvody	• Nesdílejte veřejně svou aktuální polohu ani cestovní plány. • Dávejte pozor na falešné stránky FIFA, QR kódy a neoficiální nabídky vstupenek nebo VIP služeb. • Neinstalujte neoficiální aplikace ani software související s akcí.

RYCHLÝ KONTROLNÍ SEZNAM

- Vícefaktorové ověřování (MFA) aktivováno na všech důležitých účtech
- VPN nainstalována a otestována
- Aktivováno sledování zařízení (Apple Find My, sdílení polohy přes Google Maps nebo jiné důvěryhodné služby) a možnost vzdáleného vymazání dat
- K dispozici offline kopie důležitých cestovních dokumentů
- Nastavena silná hesla nebo přístupové kódy zařízení
- Nouzové kontakty uložené offline
- Zvážena RFID ochrana pro platební karty a cestovní doklady
- Vytvořen dočasný cestovní e-mail a/nebo telefonní číslo

SIHASO

ZDROJE

Toto hodnocení bylo vypracováno na základě kombinace oficiálních vládních cestovních doporučení, pokynů v oblasti veřejného zdraví, informací o akcích FIFA, zpráv z otevřených zdrojů a osvědčených postupů v oblasti ochranných zpravodajských informací.

Government / Cybersecurity Agencies

- **CISA Travel Cybersecurity Guidance:** https://www.cisa.gov/resources-tools/resources/travel-tips
- **NSA Mobile Device Best Practices:** https://media.defense.gov/2020/Aug/18/2002473224/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF
- **NIST Cybersecurity Framework:** https://www.nist.gov/cyberframework
- **FBI Cyber Crime Prevention Guidance:** https://www.ic3.gov/PreventionAdvice
- **Europol Cybercrime Prevention Advice:** https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

Public Wi-Fi / Device Security

- **FCC Wireless and Bluetooth Security Tips:** https://www.fcc.gov/consumers/guides/wireless-connections-and-bluetooth-security-tips
- **Google Account Security Guidance:** https://safety.google/security/security-tips/
- **Apple Personal Safety and Device Security:** https://support.apple.com/personal-safety

Fraud / Scam / QR-Code Threats

- **FTC Consumer Scam Alerts:** https://consumer.ftc.gov/scams
- **FBI Warning on QR Code Scams:** https://www.fbi.gov/contact-us/field-offices/albuquerque/news/fbi-warns-of-fraudsters-using-malicious-qr-codes-to-steal-victims-money-and-personal-information
- **Interpol Cybercrime Resources:** https://www.interpol.int/en/Crimes/Cybercrime

Travel / Event Environment

- **FIFA World Cup 2026 Official Site:** https://www.fifa.com/en/tournaments/mens/worldcup/canadamexicousa2026
- **OSAC Mexico Country Security Report:** https://www.osac.gov/Country/Mexico/Content/Detail/Report

Operational Travel Security

- **NSA Best Practices for Travelers:** https://media.defense.gov/2024/May/02/2003449964/-1/-1/0/CSI_BEST_PRACTICES_FOR_TRAVELERS.PDF

SIHASO

Czech Government Resources

- **Ministry of Foreign Affairs of the Czech Republic – Mexico:** https://mzv.gov.cz/mexico

- **Czech DROZD Travel Registration System:** https://drozd.mzv.cz/
- **Czech MFA Travel Information:** https://mzv.gov.cz/jnp/cz/cestujeme/index.html
- **Czech Embassy in Mexico – Consular Information:** https://mzv.gov.cz/mexico/en/visa_and_consular_information/index.html