CESTUJTE (KYBER)BEZPEČNĚ: DOPORUČENÍ PRO CESTY DO ZAHRANIČÍ

PŘED CESTOU

1 VYUŽÍVEJTE BĚHEM CESTY „ČISTÁ“ ZAŘÍZENÍ

Pokud je to možné, vezměte si s sebou „čistá“ zařízení určená pouze pro konkrétní cestu, která neobsahují žádná vaše osobní data a důležité uživatelské účty. Může jít např. o starý telefon či tablet, který již aktivně nepoužíváte. **Pokud takové náhradní zařízení nemáte k dispozici, věnujte zvýšenou pozornost dalším doporučením.** Po návratu zařízení resetujte do továrního nastavení.

2 DŮKLADNĚ SVÁ ZAŘÍZENÍ ZABEZPEČTE

Zabezpečte zařízení novým a unikátním silným heslem/pinem, případně využijte zabezpečení otiskem prstu, nebo skenem obličeje. U důležitých služeb (e-mail, komunikační aplikace) nastavte nová silná hesla. Hesla nemějte nikde napsaná a uložená v zařízení. Kde to půjde, důrazně doporučujeme využít dvou faktorové autentizace (heslo + např. kód z SMS).

3 AKTUALIZUJTE OPERAČNÍ SYSTÉM A APLIKACE

K předejití zneužívání zranitelností u starších verzí operačního systému a aplikací doporučujeme jejich aktualizaci na nejnovější verzi.

4 ODSTRAŇTE ZE ZAŘÍZENÍ CITLIVÁ DATA

Pro případ napadení vašeho zařízení preventivně odstraňte veškerá citlivá data, informace, kontakty, fotografie a minimalizujte počet aplikací. U těch, které jsou opravdu potřeba zvažte, jaká mají nastavená oprávnění (kamera, mikrofon, galerie fotografií).

NA CESTĚ

5 VYVARUJTE SE STAHOVÁNÍ NEZNÁMÝCH ČI ZRANITELNÝCH APLIKACÍ

Pokud je nutné neznámou či zranitelnou aplikaci používat, využívejte jí jen v nejnutnějším rozsahu a chovejte se tak, jako by veškerá komunikace a vaše data mohla být odposlouchávána či ukradena. Případně zvažte využívání webové verze aplikace. **Rovněž zvažte oprávnění, která aplikacím udělujete.** Důrazně doporučujeme instalovat aplikace pouze z oficiálních zdrojů (Google Play, Apple AppStore atd.). Aktuálně zranitelnou aplikací je mj. oficiální aplikace olympijských her v Pekingu, MY2022.

6 NEPŘIPOJUJTE SE NA VEŘEJNÉ WIFI SÍTĚ

Veřejné WiFi sítě (v kavárnách, restauracích, MHD, hotelích) bez hesel, či chráněné veřejně dostupnými hesly, jsou velmi slabě zabezpečené a mohou být využity k monitorování připojených uživatelů a případně i napadení jejich zařízení. U masových akcí jako jsou olympijské hry je takové riziko vysoké.

7 PRO PŘIPOJENÍ K INTERNETU VYUŽÍVEJTE DATOVÝ ROAMING A PLACENOU VPN

K minimalizaci případného monitorování vašich aktivit na internetu během cesty doporučujeme používat mobilní data v kombinaci se službou VPN, která dále šifruje a anonymizuje váš pohyb na síti. Doporučujeme placené VPN poskytovatele, jelikož řešení poskytovaná zdarma nemusí být spolehlivá a bezpečná. V některých státech VPN ovšem nemusí vždy fungovat.

8 KE KOMUNIKACI VYUŽÍVEJTE APLIKACE S ŠIFROVÁNÍM

Pro komunikaci využívejte aplikace s tzv. „end to end“ šifrováním – v ideálním případě aplikace Signal nebo Threema, ale lze použít i WhatsApp, Apple Face Time a další. Mějte na paměti, že v některých aplikacích je nutné tuto funkci zvlášť aktivovat. **Doporučujeme minimalizovat běžné volání a SMS.**

9 VYHÝBEJTE SE PŘIHLAŠOVÁNÍ K CITLIVÝM SLUŽBÁM

Pokud to není nezbytně nutné, doporučujeme při cestě nepřistupovat k citlivým službám, jako je internetové bankovnictví, osobní účty apod. Pokud je to nutné, po návratu je vhodné změnit k těmto službám přihlašovací údaje.

10 NENECHÁVEJTE ZAŘÍZENÍ BEZ DOZORU A NEZAMČENÁ

Mějte neustále povědomí o tom, kde se nachází Vaše zařízení, a kdo k němu má přístup. Virus se do zařízení může dostat např. prostřednictvím USB ve chvilce nepozornosti, nebo i přílišnou zvědavostí (např. nalezené USB). Bezpečné nemusí být ani hotelové pokoje a trezory v pokojích, jelikož do nich mají zpravidla přístup zaměstnanci hotelů. Jedním z řešení může být použití bezpečnostních obálek s pečetí.