

CHECK-LIST PRO CESTY DO RIZIKOVÝCH ZEMÍ

Ať už jedete do země, kde lze očekávat zvýšené riziko pro vaši osobní bezpečnost, bezpečnost elektronických zařízení, která si berete s sebou anebo pro váš výzkum, ujistěte se, prosím, že jste před cestou udělali alespoň základní opatření.

Najdete je níže rozčleněná do tří základních oblastí. Relevantní jsou pro vyučující a ostatní zaměstnance, studující i badatele a badatelky UMPRUM.

Nejste-li si jisti, zda země, kam míříte, patří mezi rizikové, podívejte se na sankční mapu EU (www.sanctionsmap.eu/). Pokud se na ní vaše destinace nachází, je to spolehlivý indikátor, že je vhodné si dávat pozor. Bližší informace v češtině najdete na stránkách Finančního analytického úřadu (<https://fau.gov.cz/informacni-zdroje>).

Buďte obezřetní již při plánování cesty do takové destinace a pečlivě zvažte přínos výjezdu pro výkon Vaší práce či studia a posouzení jeho rizik. Dostáváte-li neobvykle štědrou nabídku na výjezd (stáž, konference apod.), položte si otázku, zda je to obvyklé a není očekávána „protislužba“. **Opatrnost je na místě!**

Se vstupem do akademického prostředí jste se stali osobami s přístupem k celé škále citlivých informací, které mohou být cenné pro osoby zastupující zájmy jiných států či nestátních subjektů. To z vás daleko častěji, než si možná uvědomujete, činí cíle zájmu.

Šťastnou cestu!

OSOBNÍ BEZPEČNOST

- Zaregistrujte se do systému DROZD. (<https://drozd.mzv.gov.cz/>)
- Informujte se, zda máte všechna očkování, a potřebná doplňte. (<https://centrumcestovnimediciny.cz/vseobecna-doporuceni-pred-cestou/>)
- O aktuální bezpečnostní situaci se informujte na internetových stránkách MZV. (<https://mzv.gov.cz/jnp/>)
- Zjistěte si, které lokality, čtvrti atd. jsou rizikové a vyhněte se jim.
- Ubytování volte pouze v bezpečných čtvrtích. Šetřit na úkor bezpečí se nevyplácí.
- Pokud v cizí zemi existuje mobilní aplikace, která přináší aktuální místní bezpečnostní informace, zvažte její použití (např. Izrael).
- Zjistěte si informace o kulturních zvyklostech v dané zemi, zejména pokud jde o konzumaci alkoholu a omamných látek, vhodné oblékání, omezení dovozu a vývozu do a ze země atd. (https://europa.eu/youreurope/citizens/travel/carry/index_cs.htm)
- Nikdy nenechávejte svá zavazadla bez dozoru.

KYBERBEZPEČNOST

- Ideálně si s sebou neberte žádná školní elektronická zařízení, jako jsou pracovní laptopy nebo telefony.
- Pokud výše uvedený bod vylučuje povaha Vaší cesty, na IT si zamluvte a vyzvedněte počítač, který je určen pro zahraniční výjezdy spojené s rizikem.

- Pro připojení do školních systémů, včetně emailu používejte důsledně VPN.
- Pro zabezpečení svých elektronických zařízení používejte silná hesla a pro různé účty a zařízení neužívejte totožná.
- Ujistěte se, že máte na svých elektronických zařízeních vypnuty funkce automatického připojování k Wi-Fi a připojování pomocí služby Bluetooth.
- Pokud je to možné, pořiďte si předplacenou místní SIM-kartu a nepřipojujte se do místních veřejných ani uzavřených Wi-Fi sítí.
- Do svého elektronického zařízení nikdy nepřipojujte cizí datové nosiče (USB disky, paměťové karty apod.), ani takové, které jste na místě dostali jako dar.
- Používání přihlašovacích údajů do uzavřených systémů, e-mailů, webových služeb apod. z cizího počítače je vysoce rizikové.
- Elektronická zařízení a datové nosiče nepůjčujte třetím osobám.
- Mějte svá elektronická zařízení vždy pod kontrolou, hotelový trezor není vhodným bezpečným úložištěm pro citlivá data.
- Nenabíjejte svá elektronická zařízení z USB nabíječek a kabelů, poskytnutých na letištích, v hotelech apod. Vždy používejte pouze vlastní nabíječku. Obecně, nikdy nepřipojujte do USB portu cizí zařízení, ani kabely.
- Nevozte s sebou průkazy a čipy UMPRUM.

BEZPEČNOST VÝZKUMU

- I v případě, že cestujete s vlastním počítačem, neberte si s sebou své archivy, zejména pokud obsahují dokumentaci nebo přímo výsledná díla. Zvláště zranitelné jsou informace o autorských výsledcích, které nejsou např. patentované nebo jinak registrované.
- V zemích, které nedbají ochrany duševního vlastnictví (např. Čína, Rusko či Indie), neprezentujete veřejně dosud nepublikované práce. Zejména rozpracované projekty jsou častým cílem zcizení.
- Buďte obezřetní při navazování osobních kontaktů a sdílení informací. Nenechte se vmanipulovat do kompromitující situace.
- Pokud vyhodnotíte nějakou situaci jako budící podezření, neprodleně kontaktujte odpovědného pracovníka školy anebo pracovníky IT oddělení.
- Přistupujte s maximální opatrností k tzv. zdvořilostním darům (včetně flashdisků a paměťových karet).

PO NÁVRATU

Po návratu z cesty si nechte na IT zkontrolovat ([antivir](#), [antimalware](#) atd.) svá elektronická zařízení kvůli zjištění škodlivého software nebo jiného způsobu napadení.

U cest do států s vysokým rizikem je vhodné po návratu změnit přístupová hesla k významným informačním systémům, do vnitřní sítě apod. U středně rizikových států je vhodné toto zvážit.