Tel. 1805
El. p. cert@nksc.lt
https://www.nksc.lt

INFORMACINIS BIULETENIS
KIBERNETINIO SAUGUMO REKOMENDACIJOS KINIJOS ŽIEMOS OLIMPIADOS DALYVIAMS

2022 sausio 27 d.
Vilnius

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, Lietuvos atstovams, vykstantiems į Kinijos Liaudies Respublikos (toliau – KLR) organizuojamas žiemos olimpines žaidynes, teikia rekomendacijas dėl kibernetinio saugumo rizikų:

1. **Mažiau asmeninių išmaniųjų įrenginių.** Vykstant į žiemos olimpines žaidynes rekomenduojama vežtis tik būtiniausius išmaniuosius įrenginius ir juose laikyti tik būtiniausią informaciją.
2. **Atskiri išmanieji telefonai**. Jeigu olimpiados ar vizito KLR metu reikėtų įsidiegti specialias programėles, rekomenduojama naudoti atskirus – ne asmeninius – išmaniuosius įrenginius.
3. **VPN**. Prieš kelionę į KLR rekomenduojama įsigyti ir kelionės metu visada naudoti komercines VPN paslaugas visuose įrenginiuose, kurie gali turėti prieigą prie interneto.
4. **Slaptažodžiai**. Rekomenduojama iš anksto pasikeisti visų paskyrų (socialinių tinklų, el. pašto ir pan.) slaptažodžius. Slaptažodį turi sudaryti ne mažiau 12 simbolių – didžiosios, mažosios raidės, skaičiai, specialūs simboliai.
5. **Antivirusinė programinė įranga**. Visuose įrenginiuose be išimties (*Windows, Linux, Android, IOS*, pan.). naudoti antivirusinę programinę įrangą. Pažymėtina, kad kai kurios komercinės antivirusinės įrangos paslaugos leidžia naudotis VPN paslaugomis.
6. **Sekimo programinė įranga**. Praskenuoti įrenginius dėl sekimo programinės įrangos, pvz., naudojant – https://www.safer-networking.org, https://www.malwarebytes.com. Skenavimus vykdyti periodiškai.
7. **Belaidžio tinklo prieigos taškai.** Įrenginiuose išjungti automatinius prisijungimus prie *bluetooth, wifi* (angl. auto discovery/connection). Prisijungus prie viešo belaidžio tinklo ir nenaudojant VPN paslaugos, vengti jungtis prie paslaugų ir platformų, kurioms reikalingas autentifikavimas, pvz., el. bankininkystė, socialiniai tinklai, el. paštas, pan. Rekomenduojama prie nemokamo belaidžio tinklo jungtis tik būtiniausiais atvejais.
8. **Socialiniai tinklai, el. paštas ir kitos paslaugos**. Griežtai rekomenduojama išjungti automatinį prisijungimą ir naudoti kelių faktorių autentifikavimą (prisijungimas patvirtinamas per aplikaciją ar SMS žinute) jungiantis prie *Facebook, Twitter, Google, Microsoft* ir kitų paslaugų.
9. **TOR naršyklė**. Tais atvejais, kai yra blokuojamos VPN paslaugos, naršymui internete rekomenduojama naudoti TOR naršyklę. Tačiau TOR naršyklėje nerekomenduojama jungtis prie autentifikavimo reikalaujančių paslaugų.
10. **Socialinė inžinerija**. Vengti atidaryti neaiškias nuorodas, gautas trumposiomis žinutėmis, el. paštu, pan. Visada tikrinti nuorodų autentiškumą ir prie paslaugų jungtis tik per oficialias interneto svetaines.
11. **Aplikacijų prieiga**. Išmaniuose įrenginiuose įvertinti aplikacijų prieigos teises pagal „būtina žinoti" principą ir palikti tik tas, kurios yra būtinos paslaugos vykdymui. Likusias rekomenduojama išjungti (pvz. prieigą prie duomenų, adresų knygelės, mikrofono, kameros, pan.).
12. **Grįžus iš KLR**. Patikrinti įrenginius dėl kenkėjiško kodo ir sekimo programinės įrangos, pasikeisti visų paskyrų slaptažodžius pagal 4 punkte išdėstytas rekomendacijas.