Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j. 1843/2026-NÚKIB-E/630 • BRNO • 2. ÚNORA 2026

[SITUAČNÍ PŘEHLED]

ZIMNÍ OLYMPIJSKÉ HRY 2026: LZE OČEKÁVAT VĚTŠÍ AKTIVITU ZEJMÉNA FINANČNĚ MOTIVOVANÝCH AKTÉRŮ, SPECIFICKÝM HROZBÁM ČELÍ OLYMPIJSKÝ VÝBOR, NÁVŠTĚVNÍCI, ZÁJMOVÉ OSOBY I VEŘEJNOST

SHRNUTÍ

- **Ve dnech 6. až 22. února 2026 budou v Itálii probíhat Zimní olympijské hry (ZOH 2026). Vzhledem k mezinárodnímu charakteru a vysoké publicitě akce lze očekávat zvýšený zájem řady kybernetických aktérů, zejména finančně motivovaných kyberkriminálních skupin. Nelze vyloučit (25–50 %) ani aktivitu hacktivistů či státem sponzorovaných aktérů.**
- **Výraznými hrozbami jsou phishingové kampaně, podvodné webové stránky a mobilní aplikace či QR kódy. NÚKIB doporučuje institucím i jednotlivcům v souvislosti se ZOH 2026 zachovávat zvýšenou obezřetnost při aktivitách na internetu a ochraně vlastních zařízení.**
- **Pokud Vaše instituce spadá pod zákon o kybernetické bezpečnosti, neváhejte v případě incidentu kontaktovat NÚKIB na adrese cert.incident@nukib.gov.cz, v opačných případech incident hlaste CSIRT.cz, případně Policii ČR.**
- **Součástí tohoto přehledu je také sada obecných kyberbezpečnostních doporučení, jejichž cílem je omezit potenciální kybernetická rizika spojená s návštěvou této akce.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

Zimní olympijské hry 2026 (ZOH 2026) v italském Miláně a Cortině D'Ampezzo budou probíhat ve dnech 6. až 22. února. Mezinárodní charakter a vysoká publicita akce mohou přilákat zvýšenou aktivitu kybernetických aktérů. Hrozby mohou přijít jak od státem sponzorovaných aktérů, tak i kyberkriminálních či hacktivistických skupin. Oběťmi se pak mohou stát členové olympijského výboru, zájmové osoby a instituce, návštěvníci, firmy i široká veřejnost.

NÚKIB v Česku zatím žádný incident související s letošními ZOH nezaznamenal, avšak potenciální kybernetický incident nelze vyloučit (25–50 %). Zároveň existuje reálná možnost (25–50 %) zneužití tematiky ZOH 2026 k phishingovým kampaním, a to jak před, během, tak i po skončení olympijských her. **Z toho důvodu je na místě zvýšená obezřetnost, zejména v situacích souvisejících se ZOH 2026.**

Osoby fyzicky přítomné na ZOH 2026 by měly dodržovat základní kyberbezpečnostní pravidla pro cestování (viz Příloha 1).

OLYMPIJSKÝ VÝBOR: HROZBU PŘEDSTAVUJÍ ZEJMÉNA PHISHINGOVÉ ÚTOKY NA ORGANIZACE I JEDNOTLIVCE I HACKTIVISTÉ

Mezi nejčastější a nejvýznamnější hrozby patří finančně motivované útoky prostřednictvím phishingových e-mailů a škodlivých stránek. Předpokládaná témata škodlivých příloh phishingových e-mailů mohou zahrnovat např. falešné nabídky spolupráce spojené s partnerstvím či marketingovými nabídkami.

Dále je pravděpodobné (55–70 %), že se průběh olympijských her pokusí narušit hacktivistické skupiny. Ty podnikají zejména ideologicky motivované útoky, jejichž účelem je vlastní medializace. Nejčastěji se jedná se o defacement či útoky s cílem narušit dostupnost webových stránek (DDoS). **Útoky samy o sobě však vedou pouze ke krátkodobým výpadkům služeb.**[1]

NÁVŠTĚVNÍCI: DŮLEŽITÉ JE DODRŽOVAT ZÁKLADNÍ KYBERBEZPEČNOSTNÍ PRAVIDLA PRO CESTOVÁNÍ

Návštěvníci ZOH 2026 by měli dodržovat základní kyberbezpečnostní pravidla pro cestování jako nenechávat zařízení bez dozoru a pokud možno nevyužívat veřejné nezaheslované Wi-Fi sítě (viz Příloha 1).

Nejčastěji se návštěvníci pravděpodobně setkají s finančně motivovanými kyberzločineckými útoky. K tomuto účelu je využíván zejména phishing a jeho nové a stále častěji využívané formy jako vishing (podvodné telefonáty) či smishing (podvodné SMS). Dále falešné webové stránky, podvodné aplikace nebo QR kódy.[2]

Návštěvníci by se měli mít na pozoru již při koupi vstupenek. Ty je doporučeno kupovat pouze z oficiálních stránek ZOH. [3] Zároveň je třeba dát si pozor na podvodné e-maily vyzývající k zaplacení již uhrazených vstupenek. Pro podvodné praktiky je typická snaha o vytvoření urgence k rychlému a neuváženému rozhodnutí.

VEŘEJNOST: HROZÍ FINANČNĚ MOTIVOVANÉ ÚTOKY SKRZE PHISHING A JEHO VARIANTY

I přesto, že člověk přímo nenavštíví olympijské hry, nelze vyloučit (25-50 %), že se stane obětí kybernetického útoku. Ten se opět může promítnout v podobě různých forem phishingové zprávy s tematiku olympijských her. **Jednat se například může o nabídku volných lístků na sportovní události, propagačních předmětů či přivýdělku během ZOH 2026. Zároveň lze očekávat také nárůst podvodných stránek, např. vydávajících se za oficiální živé přenosy zdarma, které pro přístup vyžadují vložení citlivých informací.** Pro zvýšení odolnosti vůči phishingu a dalším útokům zaměřeným na veřejnost doporučujeme absolvovat kybertest.

Obrázek 1: Logo ZOH 2026

Zdroj: olympijskytym.cz

ZÁJMOVÉ OSOBY A INSTITUCE: MOŽNÉ POKUSY O ŠPIONÁŽ ZE STRANY STÁTNÍCH AKTÉRŮ

Cílem kybernetické špionáže ze strany státem sponzorovaných aktérů se mohou stát vysoce exponované, významné či zájmové osoby, stejně tak jako instituce, ve kterých působí.[4]

Potenciální cíle taktéž představují i domácí neziskové organizace, které se zabývají citlivými geopolitickými událostmi.

Hlavní strategií těchto aktérů jsou cílené phishingové a spear-phishingové útoky zneužívající aktuální události, které vystupují jako zdánlivě legitimní oficiální komunikace organizátora, státních institucí, diplomatických kanálů nebo mezinárodních organizací.

PŘÍLOHA 1: ZÁKLADNÍ KYBERBEZPEČNOSTNÍ DOPORUČENÍ V SOUVISLOSTI SE ZIMNÍMI OLYMPIJSKÝMI HRAMI 2026

Dbejte zvýšené opatrnosti před phishingem

Vzhledem k povaze a významu akce lze předpokládat škodlivé aktivity v kyberprostoru, jež mohou směřovat mimo jiné vůči účastníkům akce. V minulosti byly obdobné události zneužívány k zasílání phishingových zpráv s cílem získat citlivé informace. **Před akcí i v jejím průběhu je proto třeba dbát zvýšené opatrnosti při stahování dokumentů či otevírání příloh v rámci internetové komunikace. Zejména je důležité dbát obezřetnosti při otevírání příloh či odkazů od cizích odesílatelů.** Typicky tyto útoky využívají legitimně vypadající oficiální dokumenty, jako jsou pozvánky na recepce, programy jednání či naopak zápisy a jiné výstupy podobných akcí. Dále je vhodné vždy zkontrolovat správnost e-mailové adresy odesílatele. V některých případech mohou útočníci zneužívat tzv. typo squatting, tj. obtížně rozeznatelné překlepy v e-mailové či webové adrese ke zneužití identity např. kolegy, nadřízeného nebo legitimního webu.

Vstupenky na ZOH 2026 kupujte pouze přes oficiální stránky

Při akcích této velikosti často dochází k prodeji vstupenek prostřednictvím různých internetových portálů, překupníků a neoficiálních přeprodejů. Takový nákup s sebou nese řadu rizik. Kromě finanční ztráty při nákupu falešné nebo již použité vstupenky hrozí kupujícím také zneužití osobních údajů, které mohou být dále prodány třetím stranám či použity k jiným podvodům. Dalším problémem je skutečnost, že neoficiální prodejci neposkytují žádnou záruku ani zákaznickou podporu. V případě zrušení akce tak často není možné získat náhradu. **Vstupenky je proto doporučeno zakoupit pouze přes oficiální stránky. Pouze tak může být zaručena jejich pravost a bezpečnost citlivých údajů.**

Vyvarujte se stahování neoficiálních aplikací, využívání neoficiálních webů a neuváženému skenování QR kódů

Obchody s aplikacemi mohou nabízet v souvislosti s velkými mezinárodními událostmi nové aplikace zdarma. **Často se jedná o aplikace, které nabízejí služby jako upozorňování na výsledky zápasů, online sledování událostí či sdílení praktických informací pro návštěvníky. Ve skutečnosti však mohou sloužit ke sběru citlivých údajů, šíření malwaru nebo k přesměrování na podvodné webové stránky.** V souvislosti s celosvětovými událostmi se mohou objevovat falešné webové stránky, které se vydávají za oficiální informační portály. Mohou také poskytovat prodej vstupenek, ubytovací služby nebo online přenosy. **Tyto weby jsou často využívány ke krádeži přihlašovacích a platebních údajů.** QR kódy umístěné na veřejných místech mohou také vést na falešné weby, automaticky stahovat malware nebo přesměrovat na podvodné formuláře. **Proto je doporučeno skenovat QR kódy pouze z oficiálních a důvěryhodných zdrojů, pečlivě kontrolovat URL adresy a nezadávat citlivé údaje do neověřených formulářů.**

Minimalizujte využívání veřejných Wi-Fi sítí

Veřejné sítě na letištích, v hotelech či různých restauracích a na dalších veřejných místech velmi často nedisponují dostatečným zabezpečením. Útočníkům tím poskytují potenciální příležitost sledovat vaši komunikaci a zachytávat tak kromě potenciálně citlivých informací například také přihlašovací údaje a hesla. **Je tudíž doporučeno, pokud možno tyto sítě využívat pouze okrajově, případně se skrze ně alespoň nepřihlašovat například do internetového bankovnictví nebo dalších citlivých služeb a nesdělovat skrze ně soukromé informace.** Pokud přece jen potřebujete připojení skrze takovou Wi-Fi, využívejte VPN služby. Ty zajišťují šifrování provozu a vytváří „bezpečnější tunel“ pro vaše internetové aktivity.

Pokud chcete maximalizovat své zabezpečení, preferujte datový roaming spolu s VPN a end-to-end šifrováním

Naopak nejbezpečnější variantou je využití datového roamingu. Dodatečně lze využít také některou z VPN služeb a komunikovat skrze aplikace s end-to-end šifrováním. V takovém případě se riziko narušení důvěrnosti vaší komunikace výrazně minimalizuje.

Nenechávejte svá zařízení bez dozoru a nezamčená

Dále je doporučeno nenechávat za žádných okolností svá elektronická zařízení bez dozoru, a to primárně s ohledem na možnost dalších typů kompromitace ze strany útočníka. Pokud je to však potřeba, je vždy vysoce žádoucí dané zařízení uzamknout. V tomto případě se možnosti útočníka kompromitovat zařízení snižují.

Nabíjejte svá zařízení pouze v důvěryhodném prostředí s využitím vlastních nabíjecích kabelů a adaptérů

Mobilní zařízení je doporučeno nabíjet pouze v zabezpečeném a důvěryhodném prostředí jako např. v ubytovacím zařízení. Zároveň je důležité dbát na použití vlastních nabíjecích kabelů a nevyužívat veřejných dobíjecích stanic. Nedoporučuje se rovněž používat zapůjčené nebo nalezené nabíjecí kabely a adaptéry, ani připojovat zařízení k USB portům neznámého původu. **Během pohybu ve veřejném prostředí se doporučuje využívat externí baterie (powerbanky).**

Zabezpečte svoje služby dvoufázovým ověřením

Pro případ, že ke kompromitaci nebo záchytu vaší komunikace útočníky dojde, je vhodné mít dodatečnou úroveň ochrany vámi používaných služeb ve formě dvoufázové autentizace (2FA). Tu podporuje většina služeb jako jsou e-mailové aplikace, účty na sociálních sítích či internetové bankovnictví. Použití 2FA významně minimalizuje škody, jež může útočník napáchat i v případě, že dojde ke krádeži vašich přihlašovacích údajů.

Dávejte si pozor na využívání neznámých USB disků

V rámci veřejných akcí i mimo ně je důležité být obezřetný při manipulaci s USB disky, které nepocházejí z důvěryhodného zdroje. Útočníci často využívají taktiku, kdy pohozením nebo nabídnutím neznámého USB disku obětem zavedou malware do jejich zařízení. **Doporučujeme, abyste se vyhýbali připojování USB disků, které jste našli nebo vám byly nabídnuty cizími osobami, a vždy pečlivě prověřili jakékoli externí zařízení před jeho připojením k vašemu zařízení.**

ZDROJE

[1] Greig, J. 2024. FBI: Iranian cyber group targeted Summer Olympics with attack on French display provider. Dostupné z: https://therecord.media/iran-cyber-group-targeted-paris-olympics-israel.

[2] Palo Alto Networks. 2026. Cyber Threats to Milan-Cortina 2026. Dostupné z: https://www.paloaltonetworks.com/content/dam/pan/en_US/includes/igw/unit-42-cyber-vigilance-program/cyber-threats-to-milan-cortina-2026.pdf.

[3] Český olympijský výbor. 2025. Mějte se na pozoru! Vstupenky na ZOH nakupujte pouze v oficiálním prodeji. Dostupné z: https://www.olympijskytym.cz/article/mejte-se-na-pozoru-vstupenky-na-zoh-nakupujte-pouze-v-oficialnim-prodeji.

[4]Government of Canada. 2024. Cyber threat bulletin: The cyber threat to major international sporting events. Dostupné z: https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-major-international-sporting-events.

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP:RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP:AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Zelená **TLP:GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP:CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit/Reálná možnost	*40–50 %*
Nepravděpodobně	*20–35 %*
Velmi nepravděpodobně	*0–15 %*