Všeobecné odporúčania

Preventívne pred odchodom

- zálohujte fotky, kontakty a dôležité súbory do cloudu, alebo na externý disk
- stiahnite si offline mapy (napr. cez Google Maps alebo Mapy.cz) – pomôže vám to v prípade výpadku dát
- uložte si do telefónu (aj offline) kontakty na veľvyslanectvo, policajný zbor v cieľovej krajine a číslo banky pre zablokovanie karty
- oscannujte si pas a občiansky preukaz a majte ich dostupné pre prípad ich fyzickej straty alebo odcudzenia

Ako si chrániť zariadenia na cestách

- **Neodkladajte aktualizácie** – majte vždy najnovší systém a aplikácie
- **Používajte antivírus** – chráni pred známymi hrozbami
- **Správca hesiel** – vytvára a bezpečne uchováva silné, jedinečné heslá
- **Používajte 2FA/MFA** – Dvojfaktorová autentifikácia výrazne zvyšuje bezpečnosť prístupov
- **Vypnite automatické WiFi pripájanie** – Zamedzíte pripojeniu na neznáme siete
- **Skryte Bluetooth, Airdrop a WiFi hotspot** – Znížite riziko neoprávneného prístupu do vášho zariadenia
- **Nepoužívajte verejné USB nabíjačky** – Môžu byť zneužité na prenos škodlivého kódu
- **Plaťte bezpečne** – Uprednostnite virtuálne platobné karty alebo Google/Apple Pay

Čo robiť, ak sa stanete obeťou kybernetického útoku

1. Zablokujte platobné karty
2. Zmeňte si heslá na sociálnych sieťach
3. Nahláste podvod banke
4. Nahláste zneužitie účtu sociálnej sieti
5. Sledujte svoje účty a výpisy – hľadajte neznáme transakcie
6. Zachovajte dôkazy – e-maily, SMS a screenshoty môžu pomôcť pri vyšetrovaní
7. Po návrate domov podajte na polícii trestné oznámenie

Tip na záver

Ak si nie ste istí – radšej sa spýtajte známeho informatika, alebo hľadajte informácie na oficiálnych stránkach. Podvodníci rátajú s tým, že ľudia robia rozhodnutia v strese a rýchlo. Buďte o krok vpred. Rozhodujte sa s rozvahou. Ak cítite nátlak, paniku alebo naliehavosť v komunikácii, ide s veľkou pravdepodobnosťou o pokus o podvod. Zastavte sa a overte si situáciu skôr, než zareagujete.

www.akb.sk | backoffice@akb.sk | 02 208 67 007

AKB
Asociácia kybernetickej bezpečnosti

Bezpečne na dovolenku:

Ako sa chrániť pred digitálnymi podvodmi

Letenky, ubytovanie, prenájom auta, výlety – dnes si všetko vybavíte online. No spolu s tým rastie aj riziko, že sa stanete obeťou kyberzločinu. Tu je jednoduchý návod, ako sa chrániť.

Pred dovolenkou

Ponuky dovoleniek

E-maily alebo SMS s falošnými ponukami dovoleniek

- overujte webstránky pred rezerváciou
- seriózne cestovné kancelárie podporujú bezpečný web (HTTPS, zámok v prehliadači, doména so správnym názvom)
- vyhýbajte sa stránkam s podozrivým zakončením (.xyz, .top, .live).
- neklikajte na "výhodné ponuky", ktoré vyzerajú až príliš dobre

Súťaže o dovolenku

Podvodné súťaže zamerané na zber údajov

- skontrolujte, či organizátor súťaže uvádza pravidlá, kontakt a podmienky
- neposkytujte citlivé údaje (rodné číslo, doklad totožnosti) cez verejné formuláre
- buďte obozretní pri súťažiach bez oficiálnej webstránky

Falošné rezervácie

Falošné ponuky lacného ubytovania, alebo leteniek

- Nezadávajte údaje cez odkazy z nevyžiadanej pošty
- Používajte známe portály, kontrolujte doménu, čítajte recenzie
- Uprednostnite rezervácie s možnosťou storna a vrátenia peňazí

Zmeny rezervácií

E-maily s údajnou zmenou rezervácie hotela alebo letenky

- zmeny itinerára alebo check-inu riešte iba cez oficiálnu webstránku prepravcu – nie cez odkazy v e-mailoch
- pri podozrivých výzvach na doplatenie alebo potvrdenie, kontaktujte hotel/aerolinku priamo
- platobné údaje zadávajte len na overených portáloch – nie cez odkazy v e-mailoch

Parkovanie pri letisku

Neexistujúce parkovacie služby s platbou vopred

- rezervujte parkovanie len cez stránky letiska alebo známe parkovacie portály
- overte si recenzie a polohu parkoviska na mapách
- používajte bezpečné platobné brány

Platby online

Krádež platobných údajov pri platbe cez nezabezpečené alebo falošné stránky

- plaťte len cez dôveryhodné portály a aplikácie (Google Pay, Apple Pay),
- neposkytujte platobné údaje mimo oficiálnych formulárov platobných portálov
- používajte virtuálne platobné karty s nízkym limitom
- neposkytujte fotky svojho pasu alebo občianskeho preukazu cez e-mail alebo chat
- pred platbou skontrolujte, či stránka má platný bezpečnostný certifikát (HTTPS s ikonou zámku)

Zneužitie automatických odpovedí

Zneužitie informácie o vašej dlhodobej neprítomnosti

- nastavujte automatickú odpoveď iba na pracovnej mailovej schránke
- automatické odpovede nenastavujte pre neznáme maily
- napíšte iba stručnú automatickú odpoveď bez detailov o destinácii alebo dĺžke pobytu
- neposkytujte v automatickej odpovedi mailové a telefonické kontakty, ani na iných kolegov

Na dovolenke

Podvodné miestne služby

Mobilné, alebo internetové aplikácie s ponukami falošných lokálnych služieb (ubytovacie a prepravné služby, fakultatívne výlety, návody na zľavy, vybavenie víza atď.)

- aplikácie sťahujte len z oficiálnych obchodov (Google Play, App Store),
- sledujte hodnotenia aplikácií
- v nedemokratických krajinách existuje aj možnosť, že pôjde o oficiálnu aplikáciu, ktorá zbiera osobné údaje

(Ne)bezpečné Wi-Fi siete

Verejné siete môžu viesť ku odpočúvaniu vašich prístupových údajov, alebo odcudzeniu osobných údajov

- nepoužívajte verejné Wi-Fi na citlivé operácie (internet banking, pracovný e-mail)
- ak už musíte použiť verejnú Wi-Fi, použite VPN
- uprednostnite lokálnu dátovú sieť (pred odchodom si vyberte vhodný roamingový program, alebo si na hneď po príchode na letisku kúpte eSIM)
- vypnite automatické pripájanie k sieťam

Podvodné eSIM

Falošné odkazy na eSIM s údajne výhodným dátovým balíkom, ktoré stiahnu škodlivý softvér alebo vystavia zariadenie sledovaniu

- Kupujte eSIM len z overených oficiálnych zdrojov (napr. oficiálne operátorské stránky, odporúčané appky, napr. Airalo, Holafly).
- Neklikajte na odkazy propagované cez náhodné Wi-Fi siete alebo letáky s QR

Zdieľanie dovolenky na sociálnych sieťach

Zneužitie informácie o vašej dlhodobej neprítomnosti

Počas prípravy alebo pobytu na dovolenke nezdieľajte verejne informácie o tom, kde a ako dlho sa zdržiavate. Takéto údaje môžu bytoví zlodeji využiť na plánovanie vlámania.

- zverejňujte zážitky až po návrate z dovolenky
- nastavte si súkromie
- zabezpečte dohľad nad bytom (ak nemáte EZS, požiadajte o občasný dohľad suseda, alebo niekoho z rodiny)

Zdieľanie polohy a pobytu v reálnom čase

Zneužitie informácie o vašej aktuálnej vzdialenosti od bytu

- lokality zdieľajte s oneskorením a len pre dôveryhodné osoby
- vypnite GPS ak ho práve nepotrebujete
- vopred informujte blízkych, ako vás môžu v núdzi kontaktovať - zabránite podvodníkom vydávať sa za vás

Strata alebo krádež zariadenia

Strata alebo krádež telefónu, tabletu alebo notebooku počas relaxu

- zariadenia nenechávajte bez dozoru
- zvážte použitie smart lokátorov (napr. Apple AirTag) pre lokalizáciu batožiny alebo techniky
- používajte PIN a biometrické overovanie (FaceID, odtlačok prsta)
- nastavte si šifrovanie zariadenia
- aktivujte funkciu vzdialeného vymazania
- aktivujte si PIN na ochranu SIM karty – zabránite zneužitiu cez tzv. „SIM swapping“

Zneužitie QR kódov v turistických lokalitách

Presmerovanie na podvodné weby, infiltrácia škodlivým kódom

- neskenujte QR kódy z nálepiek bez kontextu
- skontrolujte URL adresu po naskenovaní kódu
- vypnite automatické otváranie odkazov po naskenovaní

Verejné USB nabíjačky

„Juice jacking“ – prenos malvéru cez USB

- vyhnite sa nabíjaniu z verejných USB portov
- uprednostnite elektrické zásuvky
- používajte vlastné adaptéry pre USB nabíjacie káble

Falošné dotazníky a prieskumy

Falošné dotazníky v hoteloch alebo letiskách s cieľom získania kontaktov (napr. pod zámienkou súťaže alebo bonusu)

- neposkytujte údaje v iných, než oficiálnych dotazníkoch hotela alebo cestovnej kancelárie
- overte, kto anketu organizuje

Podvodné bezpečnostné správy

Phishing o „zablokovanom účte“, nutnosti „overenia prihlasovacích údajov“ alebo „súrnej aktualizácie“

- ignorujte výzvy na prihlásenie cez odkazy v správach
- prihlasujte sa len cez oficiálne webstránky alebo aplikácie
- používajte dvojfaktorové overenie

Nevyžiadané Bluetooth pripojenia

Neautorizovaný prístup cez Bluetooth

- vypínajte Bluetooth, ak ho nepoužívate
- nepotvrdzujte neznáme pripojenia
- nastavte viditeľnosť zariadenia len pre známe kontakty

Nezabezpečené hotelové zariadenia

Zdieľané verejné počítače a tlačiarne (potenciálne napadnuté malvérom)

- nepoužívajte verejné počítače na prihlásenie do e-mailov, sociálnych sietí ani bankových účtov
- po tlačení dokumentov vždy zmažte súbory zo zariadenia alebo USB
- ak potrebujete pracovať, použite vlastné zariadenie a zabezpečené pripojenie

Sociálne inžinierstvo

Manipulácia pomocou deepfake hlasových alebo video správ

- vždy si overte kontakt prostredníctvom oficiálnych kanálov
- nikdy neposkytujte heslá, prístupové údaje ani kódy cez telefón
- ak vás niekto kontaktuje „s naliehavým problémom“ (napr. problém s ubytovaním alebo bankou), zastavte sa a zatelefonujte späť na oficiálne číslo z webstránky
- vyhýbajte sa rozhodnutiam pod časovým tlakom, najmä ak ide o peniaze alebo prístupové údaje.

Kyberšikana – podceňované riziko

Nevyžiadané správy, komentáre, falošné profily, odcudzenie a zneužitie fotografií, vydieranie

Kyberšikana počas ciest môže mať rôzne formy:

- negatívne komentáre pod príspevkami
- šírenie falošných informácií o vašom pobyte či vzhľade
- vytváranie falošných profilov s vašimi fotkami
- obťažovanie cudzími osobami cez správy alebo komentáre
- zdieľajte obsah len s dôveryhodnými osobami a priateľmi
- nastavte si súkromie profilu
- v prípade útoku zablokujte útočníka a nahláste obsah platforme
- uchovajte dôkazy (screenshoty), ak sa rozhodnete podať trestné oznámenie
- pri výraznom obťažovaní zvážte kontaktovanie polície alebo odborníka na kyberbezpečnosť
- Zdieľanie zážitkov má byť pozitívne – nemá to byť dôvod na stres alebo ohrozenie

Obzvlášť zdôrazňujeme, že verejné zdieľanie fotografií detí je veľmi nebezpečným zvykom. Jednak ide narušenie súkromia detí bez ich súhlasu. Avšak zároveň ide o veľmi vážnu hrozbu zneužitia fotografií, ktorá je základom pedofilného zločinu. Rodičia by mali zvažovať, či vôbec zdieľať fotografie svojich detí na verejných profiloch. Odporúča sa obmedziť viditeľnosť príspevkov len na úzky okruh blízkych osôb.

Po dovolenke

Kontrola prístupových účtov

- po návrate domov skontrolujte všetky svoje online kontá, sociálne siete aj internet banking
- skontrolujte históriu prihlásení do e-mailu, cloudových účtov a sociálnych sietí
- uistite sa, že sa neobjavila žiadna podozrivá aktivita - ak zistíte čokoľvek podozrivé, neodkladajte reakciu
- skontrolujte si aj zoznam naposledy použitých zariadení a lokácií (napr. v nastaveniach Google alebo Facebook účtu) - ak vidíte cudzie prihlásenie, odhláste ho a zmeňte heslo
- ak ste sa počas dovolenky prihlasovali z verejného počítača (napr. hotel, internetová kaviareň), bezodkladne zmeňte všetky heslá, ktoré mohli byť uložené alebo zachytené

Kontrola zariadení

- aktualizujte antivírus a skontrolujte zariadenie pomocou bezpečnostného softvéru
- skontrolujte zoznam pripojených zariadení vo vašom Wi-Fi routeri, odstráňte cudzie WiFi zariadenia zo zoznamu a zmeňte heslo k Wi-Fi, ak máte podozrenie
- odstráňte všetky nepotrebné WiFi prístupové body zo zoznamu v mobile, tablete a notebooku
- vymažte nepotrebné aplikácie alebo dáta, ktoré ste si nainštalovali počas cestovania

Kontrola transakcií

- po návrate pravidelne sledujte výpis z účtu a aktivujte si notifikácie pri platbách
- ak nájdete podozrivú transakciu, okamžite kontaktujte