BUĎTE BEZPEČNÍ ONLINE · 01 / 25

Buďte bezpeční online.

Praktický sprievodca pre každého. Desať minút čítania. Užitočné na celý život.

PRE KOHO

Rodičov · deti · seniorov · firmy · každého online

ROZSAH

Trinásť očíslovaných krokov · približne 10 minút

Väčšinu z nás nikto online bezpečnosť neučil. Nie v škole, nie v práci. Nikde.

Keď sa potom niečo zlé stane, obviňujeme sami seba. Nemali by sme. Nikto nám predsa nepovedal, na čo si dávať pozor.

Tento sprievodca z vás neurobí odborníka na bezpečnosť. Dá vám trinásť najdôležitejších vecí, vysvetlených jednoducho.

Prečítajte si ho raz. Urobte, čo sa dá. Pošlite ho ďalej.

Môžete byť starý rodič, rodič, tínedžer alebo majiteľ malej firmy. Funguje pre všetkých.

Začnite tu.

AK STIHNETE LEN TRI VECI

01 **Nastavte si passkeys na dôležitých účtoch**

02 **Nainštalujte si správcu hesiel**

03 **Dohodnite si v rodine „bezpečné slovo“**

Urobte to a ste ďalej ako väčšina. Potom sa vráťte a prečítajte si zvyšok.

Vaše účty a heslá.

Väčšina útokov sa začína ukradnutým heslom. Tieto štyri kroky to vyriešia.

Používajte passkeys, kde sa dá.

01

Passkey je ako digitálny kľúč od domu. Žije vo vašom telefóne alebo počítači. Keď sa prihlásite, zariadenie overí, že ste to vy. Žiadne heslo, ktoré si treba pamätať. Žiadne, ktoré niekto ukradne.

Veľké služby už passkeys podporujú: Apple, Google, Microsoft, PayPal, Amazon, WhatsApp, GitHub a mnoho ďalších.

UROBTE TOTO

Keď sa vás aplikácia alebo stránka nabudúce opýta, či chcete passkey, povedzte áno.

Zapnite dvojfaktorové overenie — ale nie cez SMS.

02

Dvojfaktorové overenie (2FA) znamená dva kroky pri prihlásení. Vaše heslo plus ešte niečo. To „niečo“ bývalo kódom cez SMS.

SMS kódy sa dajú ukradnúť. Zločinci sa naučili oklamať mobilných operátorov, aby vaše číslo preniesli na svoju SIM. Volá sa to SIM swapping a stáva sa to často.

UROBTE TOTO

Použite autentifikačnú aplikáciu. Dobré bezplatné možnosti: Microsoft Authenticator, Google Authenticator, Twilio Authy. Nainštalujte si jednu a nastavte ju na dôležité účty.

Akékoľvek 2FA je lepšie ako žiadne. Ak je jedinou možnosťou SMS, aj tak ju zapnite.

Používajte správcu hesiel.

03

Ak to isté heslo používate na viacerých miestach, jeden únik sa zmení na desiatky. Ľudia heslá opakujú, lebo zapamätať si stovky je nemožné.

Správca hesiel vytvorí pre každú stránku unikátne silné heslo a pamätá si ich za vás. Vy si pamätáte len jedno hlavné heslo.

UROBTE TOTO

Nainštalujte si jeden. Dobré možnosti: Bitwarden (zdarma), 1Password, KeePassXC. Prehliadače majú tiež vstavaných správcov, no samostatné aplikácie sú bezpečnejšie a fungujú naprieč zariadeniami.

Majte zariadenia aktualizované.

04

Aktualizácie opravujú diery. Zločinci prehľadávajú internet a hľadajú zariadenia, ktoré neboli aktualizované. Sú to najjednoduchšie terče.

UROBTE TOTO

Zapnite automatické aktualizácie na telefóne, počítači aj v aplikáciách. Ak má váš Wi-Fi router viac ako päť rokov, vymeňte ho — staré routery prestanú dostávať aktualizácie a stávajú sa tichým rizikom.

Rozpoznávanie podvodov.

II

Podvody v roku 2026 vyzerajú presvedčivo. Veľmi. AI pomáha zločincom písať správy, ktoré v akomkoľvek jazyku vyzerajú seriózne. Stará rada („hľadajte gramatické chyby“) už neplatí.

Spomaľte, než kliknete alebo naskenujete.

05

Väčšina podvodných správ chce, aby ste spanikárili. „Zásielka čaká.“ „Účet bude zablokovaný.“ „Zaznamenali sme neobvyklú aktivitu.“

Trik je v naliehavosti. Ak cítite tlak konať, práve vtedy zastavte.

UROBTE TOTO

Ak vás správa nabáda kliknúť na odkaz, neklikajte. Otvorte aplikáciu alebo stránku sami — napíšte adresu do prehliadača. To isté platí pre QR kódy v parkovacích automatoch, reštauráciách a letákoch. Zločinci prelepujú skutočné QR kódy falošnými.

Naliehavé správy od „rodiny“ či „šéfa“ berte podozrievavo.

06

Toto je najstrašidelnejšia zmena posledných dvoch rokov. Zločinci dokážu naklonovať niekoho hlas z krátkeho videa na sociálnej sieti. Zavolajú vám a znejú presne ako váš syn alebo šéf — s naliehavou prosbou o peniaze. Také hovory sú presvedčivé. Nasadia sa im aj opatrní ľudia.

UROBTE TOTO

Dohodnite si v rodine „bezpečné slovo“. Obyčajné slovo, ktoré by ste nepovedali len tak. Ak niekto zavolá, že je v núdzi, požiadajte oň. Ak ho nevie, je to podvod. Zložte a zavolajte späť na číslo, ktoré máte uložené.

Pri šéfovi či kolegovi platí to isté. Overte si to kanálom, ktorému už dôverujete.

Naučte sa rozpoznať investičné podvody.

07

Najväčší finančný podvod 20. rokov má viac mien: pig butchering, romantický investičný podvod, krypto podvod. Schéma je vždy rovnaká.

01	Niekto vás osloví na sociálnej sieti alebo v zoznamke
02	Pôsobí milo, zaujímavo, úspešne
03	Týždne či mesiace budujú dôveru
04	Spomenú „skvelú investičnú príležitosť“
05	Investujete malú sumu, vidíte fiktívny zisk
06	Investujete viac. Potom ešte viac.
07	Jedného dňa sú peniaze preč.

UROBTE TOTO

Ak ktokoľvek, koho ste spoznali online — akokoľvek milo pôsobí — spomenie investičnú platformu, prestaňte s ním komunikovať. Bez výnimiek. Povedzte o tom niekomu blízkemu. Tieto podvody fungujú, lebo obete sa hanbia prosiť o pomoc.

Ochrana vašich údajov.

III

Čo uniká, čo sa zneužíva a čo môžete zdieľať bez neskoršieho ľutovania.

Zistite, či vaše údaje neunikli.

08

Firmy sa dajú nabúrať. Vaše e-maily, staré heslá a niekedy aj adresy končia v databázach, ktoré si zločinci vymieňajú a predávajú.

Existuje bezplatná služba, ktorá vám povie, čo o vás uniklo.

UROBTE TOTO

Choďte na haveibeenpwned.com. Zadajte svoj e-mail. Ak niečo uniklo, zmeňte tam heslá a zapnite passkey alebo 2FA cez autentifikátor.

Zvážte, čo zdieľate — hlas aj fotografie.

09

Každé krátke video s vaším hlasom, každá fotka vašej tváre, každý verejný príspevok z dovolenky je pre niekoho tréningový materiál. Zločinci používajú verejné klipy na klonovanie hlasu. Dovolenkové fotky im hovoria, kedy je váš dom prázdny.

Nie je to výzva všetko zmazať. Je to pripomienka, že verejné príspevky sú naozaj verejné.

UROBTE TOTO

Raz ročne skontrolujte nastavenia súkromia. Nastavte účty ako súkromné, ak chcete, aby ich videli len priatelia. Zamyslite sa pred zdieľaním hlasoviek vo verejných skupinách. Vypnite polohu na fotkách.

Pre rodiny.

IV

Tri rozhovory, ktoré sa oplatí viesť ešte predtým, než ich niekto u vás doma bude potrebovať.

Rozprávajte sa s chlapcami v puberte o sextortion.

10

Je to ťažká téma. Ale mlčanie je väčšie nebezpečenstvo.

Tínedžeri (najmä chlapci) patria v roku 2026 medzi najčastejšie terče. Niekto sa vydáva za dievča podobného veku, chvíľu si píše, pošle fotku, pýta si jednu späť — a potom vyhráža, že ju rozposle, ak chlapec nezaplatí. Obete sa hanbia. Niektorí si vzali život.

Moderné verzie používajú fotky vygenerované AI. Obeť v skutočnosti žiadnu fotku neposlala. Zločincovi je to jedno.

Povedzte im:

- Ak niekto online pýta fotku, prestaň s ním komunikovať
- Ak ti vyhrážajú, neplať. Platením to neprestane
- Správy nezmazávaj. Sú to dôkazy
- Hneď to povedz dospelému, ktorému veríš. Nebudeme sa hnevať

> **Tá časť „nebudeme sa hnevať“ je najdôležitejšia. Tínedžeri mlčia hlavne zo strachu, že prídu o telefón.**

Naučte deti: „stop, opýtaj sa, povedz.“

11

Pre deti nejde o technológiu. Ide o jednoduché pravidlo, ktoré si zapamätajú.

Ak vás niečo online pýta informácie, fotky alebo peniaze — ponúka darčeky, hry alebo tajomstvá — alebo pôsobí zvláštne, strašidelne či príliš dobre na to, aby to bola pravda:

1

Stop.

Neodpovedaj. Nekliknite. Odstúpte na chvíľu od obrazovky.

2

Opýtaj sa.

Rodiča, učiteľa alebo iného dospelého, ktorému veríš. Ukáž mu správu.

3

Povedz.

Ak to pokračuje, povedz niekomu — tomu istému alebo niekomu inému.

UROBTE TOTO

Povedzte pravidlo s dieťaťom nahlas. Nalepte si ho pri počítači. Uistite ich, že im za priznanie nezoberiete zariadenie. Práve tento strach spôsobuje, že deti mlčia.

Nezvyčajné videohovory si overte.

12

V roku 2026 zločinci dokážu falšovať video v reálnom čase. Osoba na videohovore nemusí byť tá, za ktorú sa vydáva.

UROBTE TOTO

Ak vás niekto vo videohovore žiada o peniaze, heslo alebo rýchle neobvyklé rozhodnutie, zložte. Zavolajte späť na číslo, ktoré už máte uložené. Overte si to druhým kanálom ešte predtým, než konáte.

Ešte jedna vec.

V

Keď všetko ostatné zlyhá, toto vás zachráni pred začínaním odznova.

Zálohujte to, o čo nesmiete prísť.

13

Fotky. Dokumenty. Doklady. Veci, ktoré vám budú chýbať, ak vám telefón spadne do vody alebo počítač ukradnú.

Držte sa pravidla 3-2-1.

3
Kópie
Tri kópie každého dôležitého súboru. Dve nestačia — kópia, ktorá zlyhá spolu s originálom, nie je kópia.

2
Formáty
Dva rôzne formáty: napríklad cloud plus externý disk. Rozdeľte riziko.

1
Mimo domu
Jedna kópia v inej budove alebo v cloude. Ak vám zhorí dom, fotky prežijú.

UROBTE TOTO

Väčšina telefónov a počítačov prvé dve úrovne pokryje automaticky, ak máte zapnutý iCloud, Google Drive alebo OneDrive. Skontrolujte, že to naozaj beží.

Kam sa obrátiť o pomoc.

Ak sa už niečo stalo. Alebo sa deje práve teraz.

POTREBUJETE POMOC S ČÍTANÍM?

Napíšte na **education@webnestify.org** — odpovedáme v slovenčine aj angličtine.

Na Slovensku

KYBERNETICKÁ BEZPEČNOSŤ	SK-CERT · sk-cert.sk · incidenty, phishing, kompromitácia účtov
PODVODY / VYHRÁŽKY	Miestna polícia — na podvody, vydieranie, čokoľvek trestné
FINANČNÉ ÚTOKY	Linka 24/7 vašej banky pre podvody · na zadnej strane karty
DETI A TÍNEDŽERI	Linka detskej dôvery · 116 111 · zdarma, anonymne, 24/7

V Európe

VAŠA KRAJINA	Národný CERT alebo CSIRT
ÚROVEŇ EÚ	Europol · stránka „Report Cybercrime“
SPOTREBITEĽSKÉ VECI	Európske spotrebiteľské centrum · cezhraničné podvody

Pri podozrení na sextortion mladých ľudí

ODSTRÁNENIE FOTIEK	Take It Down · takeitdown.ncmec.org · odstráni ukradnuté či AI fotky, kým sa rozšíria

Trinásť krokov. Jedna strana.

ÚČTY

01 · Používajte passkeys
02 · 2FA cez autentifikátor, nie SMS
03 · Skutočný správca hesiel
04 · Automatické aktualizácie; router starší ako 5 rokov vymeniť

PODVODY

05 · Spomaľte — adresu si napíšte, neklikajte
06 · Bezpečné slovo pri naliehavých hovoroch
07 · „Tip na investíciu“ od online známeho = odíďte

ÚDAJE A RODINY

08 · Skontrolujte sa na haveibeenpwned.com
09 · Verejné príspevky berte ako verejné; nastavenia ročne
10 · Sextortion: neplaťte, nezmazávajte, povedzte dospelému
11 · Deti: stop, opýtaj sa, povedz
12 · Nezvyčajné videohovory — zložte a zavolajte späť

OBNOVA

13 · Zálohy 3-2-1 — tri kópie, dva formáty, jedna mimo domu

Tento sprievodca je zdarma. Posuňte ho ďalej.

Zdarma na čítanie, tlač aj zdieľanie. Pošlite ho rodine. Vytlačte ho pre triedu. Preložte ho pre svoju komunitu.

Uvedenie zdroja („zdroj: Webnestify Education“) oceníme, ale nie je povinné.

Ak vám môžeme pomôcť pripraviť workshop alebo prednášku u vás v škole, radi prídeme.

PRVÉ

Vytlačte a zdieľajte

webnestify.org/stay-safe-online

DRUHÉ

Rezervujte workshop

education@webnestify.org

Webnestify Education, o. z.

Slovenské občianske združenie, ktoré sprístupňuje vzdelávanie v kyberbezpečnosti všetkým.

Sprievodcu revidujeme vždy, keď sa hrozby zmenia natoľko, aby to malo význam.

VERZIA
1.0

AKTUALIZOVANÉ
2026

LICENCIA
Zdarma

KONTAKT
education@webnestify.org