

# Čo je to digitálna stopa?



**Digitálna stopa je elektronická stopa vytvorená z dát a informácií, ktoré po sebe zanecháva každý používateľ pri každom prístupe na internet alebo k iným elektronickým zariadeniam.**

## Predstavuje digitálna stopa riziko?

Digitálna stopa sama osebe nepredstavuje riziko. Rizikové však môže byť naše narábanie s ňou. Digitálna stopa je pritom trvalá a nezmazateľná súčasť našej online existencie. Tie môžete poskytovať buď aktívne, alebo pasívne.

**Pasívnu digitálnu stopu** tvoria informácie, ktoré zanechávate v online priestore nevedome a ktoré nie sú priamo viditeľné. Napríklad typ zariadenia, ktorý používate, ako laptop či smartfón.

**Aktívnu digitálnu stopu** tvoria všetky informácie, ktoré zverejníte na internete vedome. Napríklad názory a záujmy na sociálnych sieťach alebo fotografie na Instagrame.

## Je možné digitálnu stopu ovplyvniť?

Digitálnu stopu nemá žiadny používateľ stopercentne pod kontrolou. Avšak je možné mať do istej miery aspoň tie najdôležitejšie informácie v bezpečí.

# Čo vám hrozí, keď sa nestaráte o svoju digitálnu stopu?



Spísali sme pre vás zoznam možných rizík, ktoré môžu ohroziť vaše súkromie, dáta a financie v prípade, ak sa o svoju digitálnu stopu a reputáciu dostatočne nestaráte.

1

## Poškodenie reputácie

Neslušným správaním a zverejňovaním nevhodného obsahu na internete si môžete v budúcnosti skomplikovať napríklad pracovný pohovor.

5

## Stalking

Pre „stalkerov“ a „kyberstalkerov“ je čoraz ľahšie špehovať svoje obete fyzicky, ale aj online. Internetoví používatelia dnes bežne zdieľajú súkromné údaje s kýmkoľvek a kdekoľvek.

2

## Krádež identity

Kybernetickí útočníci si na základe vašej digitálnej stopy vedia o vás vytvoriť dokonalý obraz a ukradnúť vám identitu v priebehu pár minút.

4

## Sharenting

Tento pojem pochádza z anglických slov share – zdieľať a parenting – rodičovstvo. Rodičia zverejňujú informácie o svojich deťoch a ich aktivitách na sociálnych sieťach. Tie končia nielen v rukách veľkých technologických spoločností, ale aj v rukách kybernetických zločincov či online predátorov.

3

## Krádež osobných údajov

Služby, v ktorých ste v minulosti zanechali svoju digitálnu stopu, mohli byť napadnuté útočníkmi. Prípadne mohli zaniknúť a vaše údaje mohli byť predané majiteľom, ktorých zábery nemusia byť vždy úplne čestné. Osobné údaje vám môžu ukradnúť aj z profilov na sociálnych sieťach.

# Ako chrániť vlastnú digitálnu stopu?



1

Buďte vždy slušný. Nikdy neviete, kto je na druhej strane.

2

Nastavte si súkromie vašich profilov na sociálnych sieťach tak, aby boli viditeľné len pre schválených priateľov.

3

Uskutočnite bezpečnostný audit vašich účtov na sociálnych sieťach a skontrolujte si nastavenie súkromia v službe Google.

4

Nezdieľajte vaše osobné údaje a prihlasovanie informácie prostredníctvom e-mailu, SMS správy alebo četu.

5

Zrušte účty vo všetkých službách, ktoré nepoužívate.

6

Vypnite si sledovanie polohy v aplikáciách, pri ktorých to nie je potrebné.

7

Pre každú službu používajte jedinečné heslo.

8

Nezdieľajte vaše osobné údaje a prihlasovanie informácie prostredníctvom e-mailu, SMS správy alebo četu.

9

Každé zariadenie, ktoré pripájate k internetu, chráňte bezpečnostným softvérom.