

# Čo je blacklist

Last updated 5 februára, 2025

Blacklist v kontexte e-mailového marketingu je zoznam e-mailových adries, IP adries alebo [domén](#), ktoré sú označené ako zdroje [spamu](#) alebo nežiadúcej aktivity.

Ak sa e-mailová alebo IP adresa dostane na blacklist, znamená to, že e-maily odosielané z tohto zdroja môžu byť blokované alebo automaticky presmerované do zložky nevyžiadanej pošty (spam) príjemcovými e-mailovými servermi.

Blacklisty sú bežne používané poskytovateľmi e-mailových služieb na ochranu používateľov pred spamom a phishingovými útokmi.

## Typy blacklistov – verejné a súkromné

Existujú dva hlavné typy blacklistov – verejné a súkromné:

- súkromné blacklisty si tvorí a spravuje každá organizácia alebo e-mailová služba podľa vlastných kritérií
- verejné blacklisty sú zdieľané naprieč rôznymi službami a poskytovateľmi

Verejné blacklisty spravujú antispamové organizácie a bezpečnostné spoločnosti a bývajú aktualizované pravidelne na základe aktivít, ktoré ich prevádzkovatelia identifikujú ako potenciálnu hrozbu.

Dostať sa na verejný blacklist je preto pro odosielať a nepríjemnejšie.

## Ako sa váš e-mail na blacklist dostane?

Vaše e-mailová adresa sa môže dostať na blacklist z rôznych dôvodov, napríklad ak:

- odosielate veľké množstvo e-mailov, ktoré používatelia označujú ako spam
- používate neoverené zoznamy kontaktov (nakupujete kontakty)
- odosielate správy bez súhlasu príjemcov (opt-in)

- váš e-mail napadnú hackeri a zneužijú ho na šírenie spamu alebo phishingu

## Dôsledky umiestenia na blacklist

Ak je vaša adresa na blacklist, môže sa stať, že vaše e-maily **budú rovno označené ako spam** alebo príjemcom vôbec nebudú doručené.

To môže **významne poškodiť povest' vašej značky** a negatívne ovplyvniť výsledky e-mailových kampaní.

## Ako sa z blacklistu dostať

1. Najskôr zistite, na akom konkrétnom blackliste sa nachádzate (môžete využiť verejné nástroje, ako je [MXToolbox](#) alebo [DNSBL](#)).
2. Skontrolujte, či sú vaše e-maily v súlade s [bežnou e-mailovou praxou](#).
3. Ak máte podozrenie z možného hacknutia alebo zneužitia svojho e-mailového účtu, kontaktujte svojho poskytovateľa (ten spravidla sám automaticky deteguje podozrivú aktivitu na vašom účtu).
4. Svoj účet pre istotu zabezpečte [dvojfaktorovou autentifikáciou](#).
5. Akonáhle uskutočníte nápravné kroky, môžete priamo kontaktovať správcu blacklistu a požiadať o odstránenie. Niektoré blacklisty majú online formuláre, kde môžete doložiť nápravu, iné vyžadujú priamu komunikáciu.