Čo je e-mail spoofing

Last updated 17 apríla, 2026

E-mail spoofing je oklamanie odosielateľa e-mailu tak, aby správa vyzerala, že pochádza od dôveryhodnej osoby alebo firmy. Útočník upraví pole odosielateľa *From:* tak, aby príjemca videl známu adresu, aj keď e-mail v skutočnosti prišiel z iného serveru.

E-mail spoofing je bežnou súčasťou phishingu a podvodných kampaní.

Ako e-mail spoofing funguje

mailový protokol SMTP historicky umožňuje nastaviť odosielateľa pomerne voľne. Ak doména nemá správne nastavené ochranné mechanizmy, je možné uviesť inú adresu, než odkiaľ bol e-mail skutočne odoslaný. Útočník tak môže:

- odoslať e-mail zo svojho serveru
- nastaviť falošnú adresu odosielateľa
- vydávať sa za banku, kolegu alebo dôveryhodnú firmu

Bez ochranných technológií môže takýto e-mail prejsť až do doručenej pošty.

Prečo je e-mail spoofing nebezpečný

Nebezpečenstvo sa skrýva v tom, že príjemca dôveruje zobrazenej adrese odosielateľa. To môže viesť napríklad k:

- odoslaniu peňazí podvodníkovi
- vyzradeniu prihlasovacích údajov
- inštalácii škodlivého softvéru
- poškodeniu reputácie firmy

Spoofing je technický prostriedok, ktorým útočník zvyšuje dôveryhodnosť podvodu.

Ako sa pred e-mail spoofingom brániť

Ochrana spočíva v správnej konfigurácii e-mailových bezpečnostných mechanizmov.

Základ tvorí:

- ***SPF*** *– určuje, ktoré servery môžu odosielať e-maily za danú doménu*
- ***DKIM*** *– pridáva digitálny podpis e-mailu*
- ***DMARC*** *– stanovuje pravidlá, čo robiť pri zlyhaní overenia*

Kombinácia všetkých spomenutých technológií výrazne znižuje riziko zneužitia domény.

E-mail spoofing vs. phishing

E-mail spoofing je technika oklamania identity. Phishing je konkrétny typ útoku, ktorý túto techniku často využíva. Spoofing teda nie je samotný cieľ, ale nástroj k tomu, aby podvodný e-mail pôsobil dôveryhodne.

*Prečítajte si článok**Phishingové e-maily – ako ich spoznať a ako sa pred nimi brániť?*