

OD PHISHINGU K MODERNÉMU RIADENIU RIZÍK S TREND MICRO

KYBERNETICKÁ BEZPEČNOST V PRAXI 5.0



sicurio>_



Filip Marvan

Sr. Solutions Engineer Trend Micro



Marek Majka,

CEO Sicurio sr.o.

„Phishing“

STARÁ HROZBA / NOVÉ TRIKY / ROVNAKÝ CIEĽ

1995



2026



sicurio>_



Traditional Phishing
(E-mail)



Spear Phishing
(Cílený)



Smishing
(SMS Phishing)



Whaling
(Lov na veľryby)



Angler Phishing
(Sociálne siete)



Vishing
(Voice Phishing)



Quishing
(QR Phishing)



Pharming

„Prečo je stále tak úspešný?“

KLÚČE ÚSPECHU PHISHINGU

1

Cenovo dostupný a technicky nenáročný

Phishing nevyžaduje drahú infraštruktúru ani pokročilé hackerské schopnosti. Útočník vie s minimálnymi nákladmi rozposlať tisíce správ a čakať, kto sa chytí.

2

Útočí na človeka, nie na technológiu

Phishing zneužíva emócie ako strach, zvedavosť, autoritu a časový tlak. Aj dobre zabezpečená firma môže zlyhať, keď útočník presvedčí človeka, aby klikol alebo prezradil údaje.

3

Vysoká úspešnosť pri nízkom riziku

Aj keď uspeje len malé percento správ, pri masovom rozosielaní to útočníkom stačí. Z ich pohľadu ide o veľmi výhodný model: malá investícia, veľký dosah, slušná návratnosť.

4

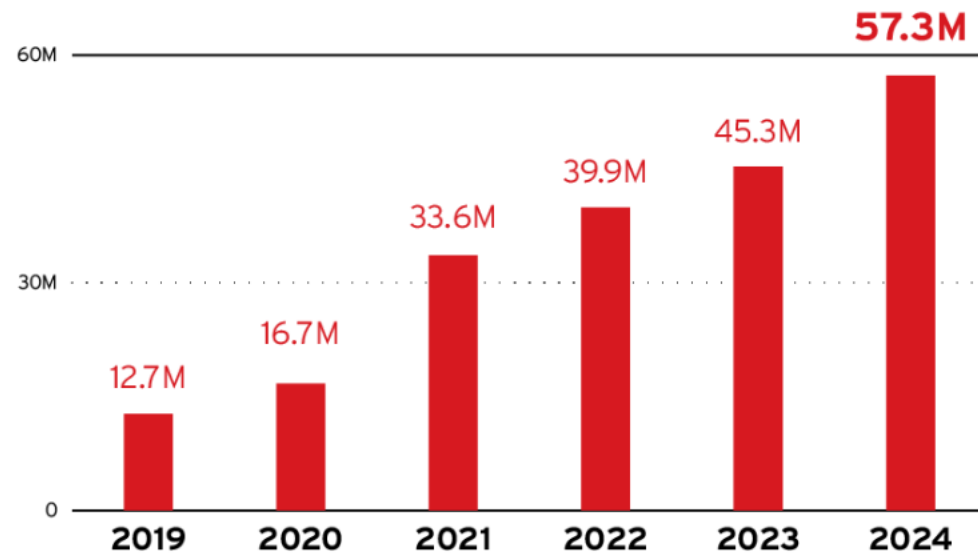
AI zrýchľuje a zlepšuje tvorbu útokov

Vďaka AI vedia útočníci rýchlo pripraviť presvedčivé e-maily, SMS správy, falošné texty aj personalizovaný obsah bez chýb. To zvyšuje dôveryhodnosť aj objem útokov.

„Štatistiky phishingu z globálneho pohľadu“

OBLÚBENEC HACKEROV

- **Finančný dopad:** Celosvetovo dosiahol finančný dopad phishingových útokov v roku 2024 odhadovaných **3,5 miliardy dolárov**.
- **Nárast útokov:** Phishingové útoky sa za 5 rokov zvýšili o viac ako **350%**, čo z nich robí jednu z najrýchlejšie rastúcich kybernetických hrozieb.
- **Dominancia e-mailov:** E-mail zostáva najbežnejším vektorom útokov a predstavuje viac ako **65 %** všetkých phishingových pokusov.
- **Rastúca miera úspešnosti:** Miera úspešnosti útokov sa vyšplhala na **18 %**, alarmujúci trend naznačuje čoraz vyššiu úspešnosť obchádzania bezpečnostných opatrení a manipulácii s obeťami.
- **Cielom sú heslá:** Viac ako **70 %** útokov sa zameriava na krádež prístupových opravení vďaka ktorým útočníci získajú neoprávnený prístup k podnikovým sieťam a citlivým údajom



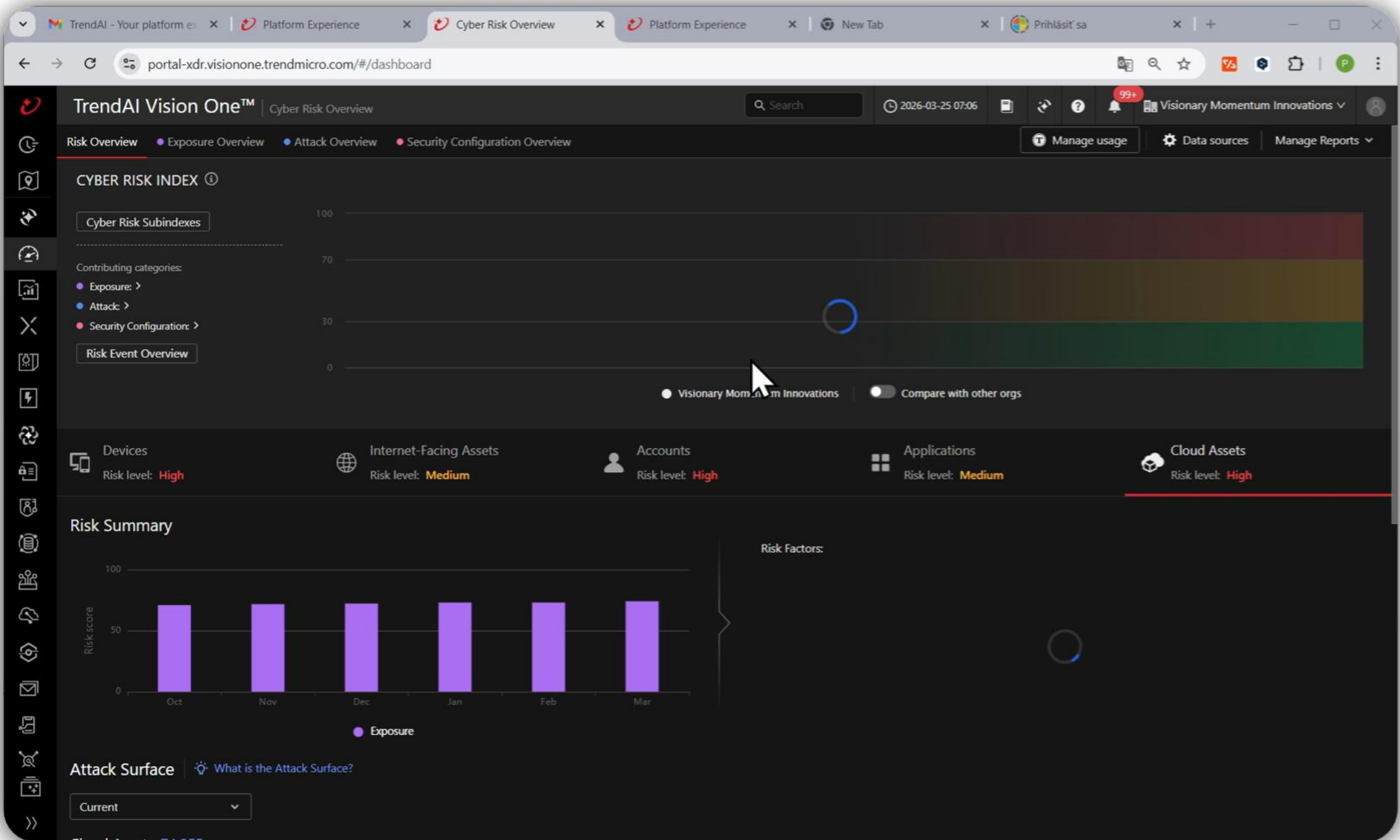
©2025 TREND MICRO

Figure 1. Detected high risk threats after Microsoft 365 and Google Workspace from 2019 to 2024

„SLOVENSKO & phishing“

TAKTIEŽ SME V HĽADÁČIKU KYBERZLOČINCOV

- 2024 NBÚ uvádza že phishing zostáva dlhodobo najrozšírenejšou a najúspešnejšou formou útoku.
- 2022 NBÚ upozorňoval na rastúci trend phishingových kampaní a narastajúcu sofistikovanosť útokov. Správa spomína zneužívanie geopolitických tém, skracovačov URL, aj prvé zneužívanie ChatGPT na tvorbu phishingových e-mailov.
- 2023 phishing je najčastejším vstupným vektorom útoku. NBÚ uvádza, že dominovalo vydávanie sa za kuriérske služby, banky, finančné inštitúcie, políciu, Interpol aj štátne authority.
- 2024 NBÚ opisuje phishingové kampane proti zamestnancom verejnej správy a kompromitované e-mailové účty používané na ďalšie šírenie phishingu.
- CSIRT.SK vo svojich mesačných správach opakovane uvádza, že v bežnej operatívnej rieši najmä phishingové kampane, pričom phishing je dlhodobý a nie jednorazový problém.



„REPORT phishingu“

ZA KAŽDÝM KLIKNUTÍM SÚ DÁTA



/ Závěrečná správa

II. PHISHINGOVÁ KAMPAŇ - REPORT


SOMI Systems a.s.
Lazovná 69
974 01 Banská Bystrica
Slovenská republika

22/12/2025

From: Microsoft Account Team <microsoft@microsoft.accountteam.com>
Subject: Platnosť vášho hesla čoskoro vyprší - Microsoft Outlook

To: Marek
[View this email in your browser](#)

Podhodnená emailová adresa
microsoft@microsoft.accountteam.com s vymyslenou doménou v tvare **@microsoft.accountteam.com**.



Účet používateľa: marek.majka@sicurio.sk

Podhodnený email nespĺňa štandard oficiálnej komunikácie spoločnosti Microsoft (chýbajúce logo).

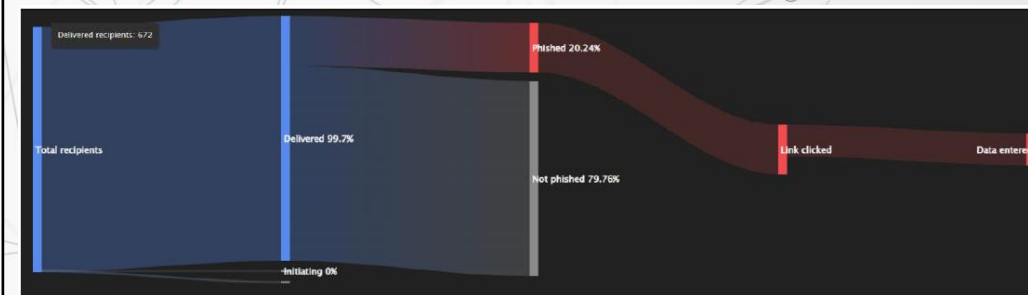
Dobrý deň, Marek.

Platnosť hesla pre váš účet marek.majka@sicurio.sk čoskoro vyprší, na obnovenie prístupu k e-mailu, kontaktom, súborom a funkciam kalendára je potrebné ho znova overiť. Ak chcete aktualizovať svoj účet marek.majka@sicurio.sk postupujte podľa krokov uvedených nižšie.

- 1 [Prihláste sa do vášho účtu](#)
- 2 Zadať vaše súčasné heslo.
- 3 Vaše konto bude aktualizované.

Odkazovanie na webovú stránku:
<https://cloud.phishinsight.trendmicro.com/api/lps/preview/e57416fe-872d-4390-b4db-175ae6b7ce35>
namiesto oficiálnej stránky spoločnosti Microsoft.

Ďakujeme, podpora spoločnosti Microsoft.



<p>Delivered / Total recipients</p> <p>99.7% (672/674)</p>	<p>Mail opened</p> <p>4.61% (31/672)</p>	<p>Bounced</p> <p>0.3% (2/674)</p>
<p>Phished</p> <p>20.24% (136/672)</p>	<p>Link clicked</p> <p>136 recipients</p>	<p>Data entered</p> <p>87 recipients</p>

OD PHISHINGU K MODERNÉMU RIADENIU RIZÍK S TREND MICRO

KYBERNETICKÁ BEZPEČNOSŤ V PRAXI 5.0



sicurio>_



Marek Majka,
CEO Sicurio sr.o.

t: +421 910 262 989

m: marek.majka@sicurio.sk

w: www.sicurio.sk