**GPT dirbtinio intelekto modelių taikymas smišingo atakų Lietuvoje analizei**

Lietuvoje smišingo (angl. smishing) atakos tampa vis dažnesnės, keliančios grėsmę tiek asmenims, tiek organizacijoms. Dirbtinio intelekto evoliucija suteikia papildomų galimybių apsisaugoti nuo šių kylančių grėsmių kibernetinėje erdvėje. Procrafta atliko trijų „OpenAI“ modelių palyginimą – GPT-3.5, GPT-4 ir GPT-4o – ir įvertino jų gebėjimą analizuoti smišingo pranešimus lietuvių kalba, atsižvelgiant į pranešimo siuntėją ir turinį. Naujasis GPT-4o modelis jau pasižymėjo kaip greičiausias ir tiksliausias iš GPT modelių šeimos, todėl galėtų būti itin perspektyvus įrankis kovai su smišingo atakomis Lietuvoje.

**Rizikos lygiai**

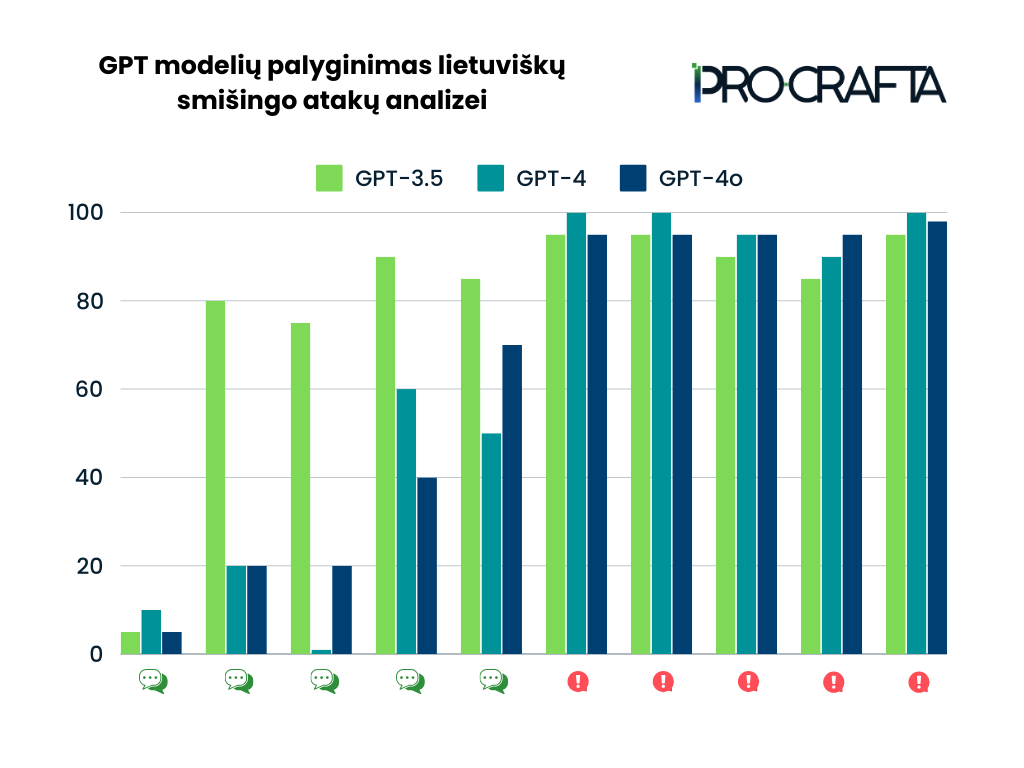
Modeliai vertina pranešimus 100 balų skalėje, priskiriančioje šiuos rizikos lygius:

* 0–20: Labai žemas rizikos lygis;
* 21–40: Žemas rizikos lygis;
* 41–60: Vidutinis rizikos lygis;
* 61–80: Aukštas rizikos lygis;
* 81–100: Labai aukštas rizikos lygis.

**Vertinimo kriterijai**

Atliekama analizė remiasi bendruoju GPT modelių supratimu apie smišingo atakas, nuoroda SMS pranešimo turinyje, panašumu su žinomais atakų scenarijais, tokiais kaip siuntų pranešimai, pranešimai iš banko, pranešimai apie baudas, mokesčiai ir kiti.

**Vertinimo rezultatai**



GPT-3.5 modelis buvo labai kritiškas beveik visų pranešimų atžvilgiu, įskaitant ir nesukčiavimo pranešimus. GPT-4 modelis pasižymėjo didesniu tikslumu nei GPT-3.5, tačiau GPT-4o modelis pranoko abu pirmtakus. GPT-4o modelis ne tik buvo greičiausias, bet ir tiksliausias, rodydamas pranašumą atliekant sudėtingas užduotis lietuvių kalba. Visais atvejais sukčiavimo pranešimai buvo įvertinti kaip aukštos rizikos.

**Išvados**

Remiantis atlikta analize, aiškiai matoma, kad naujasis GPT-4o modelis pasižymi didžiausiu tikslumu atpažįstant smišingo pranešimus lietuvių kalba. Todėl jis yra ypač naudingas praktiniam pritaikymui kibernetinio saugumo srityje. Palyginti su ankstesnėmis versijomis, GPT-4o modelis geba tiksliai identifikuoti aukštos rizikos sukčiavimo pranešimus ir juos atskirti, padedant efektyviai atpažinti sukčiavimo atvejus ir užtikrinti aukštesnį apsaugos lygį. GPT-4o modelio integravimas į esamas kibernetinio saugumo sistemas Lietuvoje gali reikšmingai padidinti apsaugos nuo smišingo atakų efektyvumą, suteikiant pažangią priemonę kovai su šia sparčiai plintančia kibernetinės grėsmės forma.

***Apie Procrafta***

*Procrafta yra informacinių technologijų plėtros ir tyrimų įmonė, įsikūrusi Klaipėdoje, Lietuvoje. Įkurta 2020 metais, Procrafta specializuojasi: duomenų analitikoje, taikomųjų dirbtinio intelekto sprendimų ir verslo valdymo sistemų kūrime.*

**Kontaktinis asmuo:**

Julita Janulė  
Direktorė  
Procrafta  
+370 684 74753  
julita@procrafta.com