

Tobulėjant technologijoms nuo pažangos neatsilieka ir sukčiai bei jų apgavysčių įrankiai. Viena naujausių šiandieninių grėsmių – dirbtinio intelekto programa „FraudGPT“. Apie tai, kaip veikia ši priemonė ir kaip apsaugoti savo pinigus nuo ją naudojančių asmenų, pasakoja „Luminor“ banko sukčiavimo rizikos valdymo skyriaus vadovas Linas Sadeckas.

Kas yra „FraudGPT“

Dirbtinis intelektas yra sistema, galinti atlikti užduotis, kurioms paprastai reikia žmogaus intelekto. Ji gali suprasti natūraliai vartojamą kalbą, priimti sprendimus, mokytis iš patirties. Tačiau anot eksperto, ji gali būti pasitelkta ir nusikaltimams vykdyti.

„FraudGPT“ yra dirbtinio intelekto pokalbių robotas, panašus į plačiau žinomą „ChatGPT“. Abi programos kuria tikrovišką ir nuoseklų turinį pagal vartotojo užklausą. Skirtumas tarp jų toks, kad paprašytas sugeneruoti apgaulingą turinį „ChatGPT“ tai daryti atsisakys, o „FraudGPT“, deja, būtent tam ir buvo sukurtas. Todėl finansiniai nusikaltėliai gali pasinaudoti šiuo robotu ir kurti įtikinamus pranešimus, jais priversti imtis veiksmų, kurių paprastai nesiimtume“, – sako ekspertas.

Anot L. Sadecko, šiandien „FraudGPT“ geba sukurti apgaulingus el. laiškus, ruošti telefonines žinutes, itin tikroviškas interneto svetaines – taip vartotojas įtikinamas atskleisti asmeninę informaciją ar savo finansinius duomenis.

Padedami „FraudGPT“ sukčiai taip pat gali sukurti ir suklastotus dokumentus, sąskaitas faktūras, mokėjimo prašymus, apgaulingus pranešimus. Neapdairiai spustelėjus pastaruosiuose esančias nuorodas ar priedus, vartotojo įrenginiai gali būti užkrečiami kenkėjiškomis programomis.

Kaip nuo „FraudGPT“ apsaugoti save ir savo pinigus

Pasak L. Sadecko, pirmas žingsnis finansiškai apsisaugoti nuo „FraudGPT“ – išsiugdyti kuo didesnę skepticizmą neiप्रastiems pranešimams.

„Nors „FraudGPT“ kuriamas turinys ir gali skambėti kaip tolimesnė grėsmė, tikėtina, kad su ja susidursime vis dažniau. Įpraskite rimtai suabejoti kaskart gavę netikėtą prašymą pateikti informaciją ar pervesti pinigus, net jeigu šaltinis iš pirmo žvilgsnio atrodo patikimas. Tikrinkite juos oficialiose interneto svetainėse ir tiesioginiais kontaktiniais būdais“, – pataria banko atstovas.

Be to, apgaulinguose tekstuose galima pastebėti ir tam tikrų anomalijų, kurios rodo bandymus sukčiauti – tai gali būti gramatinės klaidos ar neįprasti terminai, mat dirbtinis intelektas dar nėra toks pažangus, kad tokių atvejų intuityviai išvengtų.

Dar vienas patarimas, siekiant apsisaugoti nuo „FraudGPT“ keliamų grėsmių – patiems domėtis naujausiais dirbtinio intelekto įrankiais.

„Gan paprastas būdas pažinti dirbtinio intelekto įrankius – patiems juos išbandyti. Žinoma, tą reikėtų daryti apdairiai, neatskleisti asmeninės informacijos ir panašių duomenų. Tačiau praktiškai pamatę, kaip veikia anksčiau minėtas „ChatGPT“, lengviau atpažinsite jo ar kitos panašios programinės įrangos generuojamą turinį“, – sako ekspertas.

Taip pat, pataria L. Sadeckas, niekada ir niekam neatskleiskite informacijos apie savo prisijungimus prie interneto banko, slaptažodžius ar kitus konfidencialius duomenis. Jei įtariate, kad visgi susidūrėte su sukčiavimu, praneškite apie tai policijai portale „ePolicija“, paskambinę 112 ar atvykę į artimiausią policijos komisariatą.

„O jeigu įtariamas sukčiavimo atvejis, su kuriuo susidūrėte, susijęs su bankininkyste arba atskleidėte savo prisijungimus prie interneto banko ar slaptažodžius, taip pat kuo skubiau susisiekit su savo banku. Skubiai reaguodami į galimą grėsmę galite padėti ne tik sau, bet ir kitiems“, – teigia L. Sadeckas.

