*Pranešimas žiniasklaidai  
2025 m. lapkričio 14 d.*

**Dirbtinis intelektas – naujas sukčių įrankis: kaip nepakliūti į išmanią apgavystę?**

**Atvėsus orams ir ilgėjant vakarams, vis daugiau laiko praleidžiame prie ekranų. Deja, šį laiką išnaudoja sukčiai, kurie vis dažniau į pagalbą pasitelkia naujausias technologijas bei dirbtinį intelektą (DI). Jie stebi mūsų įpročius, emocijas ir aktualijas, kad rastų lengviausią kelią prie mūsų piniginių. Ekspertai įspėja – šaltasis sezonas kibernetiniame pasaulyje niekada nebūna ramus, tad turime išlikti itin budrūs.**

„Šaltuoju sezonu žmonės mažiau išeina į lauką ir daugiau lindi savo elektroniniuose prietaisuose, tuo pačiu daugiau perka – tai automatiškai didina sukčiavimo atvejų riziką. Ypač šventiniu laikotarpiu žmonės būna labiau atsipalaidavę bei emociškai pažeidžiami ir tai palengvina sukčių darbą”, – sako VILNIUS TECH Skaitmeninės gynybos kompetencijų centro direktorius Vitalijus Gurčinas.

**Pasitelkia emocijas ir tendencijas**

Technologijos keičia visą pasaulį, kartu ir sukčiavimą bei jo metodus. Sukčiai vis dažniau pasitelkia dirbtinį intelektą, kuris padeda rasti vis išradingesnius sukčiavimo metodus.

„Nors metodai išlieka tie patys – skambučiai, trumposios žinutės ir elektroniniai laiškai, siūlantys išspręsti problemas, susijusias su banko duomenimis ar pirkimais, pačios sukčiavimo schemos dažniausiai eina koja kojon su tendencijomis ir aktualijomis. Jeigu tai mokesčių deklaravimo periodas, sukčiai tai panaudos ir tuo remsis kurdami apgavystę. Toks tendencijų naudojimas dažnai veikia net ir tuos, kurie mąsto kritiškai”, – pasakoja ekspertas.

Sukčiams lengviau pasiekti žmones per emocijas, tad jie neretai pasinaudoja informacija, kurią apie žmones randa internete ir socialiniuose tinkluose. Anot V. Gurčino, kai kurie apgavikai apsimeta, jog atlieka viešas apklausas ir taip surenka asmeninę informaciją apie potencialias aukas.

**Dirbtinio intelekto panaudojimas**

Dirbtinio intelekto pagrindu sukčiai kuria įvairius atvaizdus, maketavimo elementus, taip pat istorijas ir netgi gali panaudoti DI teikiamus sprendimus, situacijas.

„Grėsmingas ne tik techninis panaudojimas, bet ir duomenų bazės pasitelkimas. DI turi informacinę bazę, kuri gali parodyti veiksmingiausius sukčiavimo metodus bei pagal tai padėti kurti efektyvesnes schemas. Jis suranda informaciją, kuri patalpinta ne tik spaudoje, bet ir moksliniuose straipsniuose, įvairiuose forumuose. Įsivaizduokite kaip galima būti pasiruošus savo žiniomis nugalėti sukčius, už kurių nugaros pasaulinio lygio sukauptų žinių bazė”, – pasakoja V. Gurčinas.

**Apsisaugoti – vis sunkiau**

Pasak akademiko, su laiku atpažinti dirbtinio intelekto panaudojimą bus vis sunkiau ir sunkiau. Tad norint išvengti sukčių pinklių, reikėtų vertinti kiekvieną situaciją kritiškai bei vadovautis esminėmis saugos taisyklėmis – neviešinti jautrių asmeninių duomenų, nevesti banko sąskaitos duomenų įtartinose nuorodose, naudoti banko apsaugas ir neatidaryti įtartinų nuorodų bei laiškų.

„Šiai dienai mes turime itin didelį informacijos srautą ir technologinių sprendimų pasiūlą, tad susidūrus su įtartinais laiškais ar žinutėmis reikėtų visų pirma patikrinti informaciją. Tai galima padaryti pasitelkiant dirbtinį intelektą ir užduodant kelis klausimus dėl įtartinos situacijos.

Taip pat svarbu atkreipti dėmesį, kad dažniausiai didelės įmonės ar pardavėjai patys neateina siūlyti prekių už itin gerą kainą ar nemokamai, norint apsipirkti reikia nueiti į internetinę svetainę ir tai padaryti pačiam. Tad bet kokie skambučiai ar laiškai su siūlymais pirkti ir įrašyti savo banko duomenis – automatiškai turėtų kelti įtarimą”, – sako Skaitmeninės gynybos kompetencijų centro direktorius.

Ekspertas papildo, kad atliekant įvairius procesus skaitmeninėje erdvėje kiekvieną sprendimą reikėtų priimti apgalvotai ir neskubant. Jeigu pardavėjas ragina pirkti greičiau, skubiai suvesti asmeninius, jautrius duomenis – tai turėtų kelti įtarimą. Jei vis dėlto nepavyksta išvengti apgavysčių, verta pagalvoti apie galimybę apsidrausti nuo sukčių.

Draudimo bendrovės BTA draudimo produkto vadovas Ramūnas Jusas pastebi, kad vis daugiau nuo sukčių nukentėjusių žmonių kreipiasi pagalbos į draudimo bendrovę. Tokie atvejai rodo ne tik augantį sukčiavimo mastą, bet ir žmonių sąmoningumą – jie vis dažniau domisi galimybe apsidrausti nuo rizikos.

„Vienas iš mūsų klientų gavo žinutę apie tariamai užlaikytą siuntą. Paspaudęs nuorodą ir suvedęs duomenis jis netrukus pastebėjo, kad iš sąskaitos dingo 300 eurų. Kitas asmuo, bandęs parduoti stalą per socialinius tinklus, sulaukė tariamo pirkėjo, kuris atsiuntė fiktyvią siuntų tarnybos nuorodą. Vos keliais paspaudimais jis neteko 1,6 tūkst. eurų. Tai klasikiniai pavyzdžiai, kai emocijos ir skubėjimas leidžia sukčiams pasiekti savo tikslą“, – pasakoja R. Jusas.

Šie klientai buvo apsidraudę ir už patirtus nuostolius gavo kompensaciją. „Dažnai žmonės net nežino, kad tokie atvejai gali būti draudžiami. Draudimas dengia ne tik pinigų praradimą dėl netikrų el. laiškų ar SMS su apgaulingomis nuorodomis, bet ir atvejus, kai sukčiai išvilioja pinigus telefonu, prisidengdami bankų, kurjerių ar net artimųjų vardu“, – sako BTA draudimo produkto vadovas.