

SKAITMENINĖ SAVIGYNA

Praktinis Vadovas, Kaip Apsisaugoti Nuo
Šiuolaikinių Grėsmių



Spear Phishing (apgaulingas susirašinėjimas)

Jei įprastas phishing yra platus tinklas, metamas į visą ežerą, siekiant pagauti bet kokią žuvį, tai spear phishing yra harpūnas, nutaikytas tiesiai į jus. Tai personalizuota, kruopščiai paruošta ir dėl to kur kas sunkiau atpažįstama apgaulė.

Užuot siuntę tūkstančius vienodų laiškų, sukčiai atlieka namų darbus, išanalizuoja konkretų taikinį (asmenį ar įmonę) ir sukuria žinutę, kuri atrodo neįtikėtina autentiška ir skirta tik jums.

Ši ataka susideda iš kelių etapų:

Taikinio Pasirinkimas: Sukčiai išsirenka aukštos vertės taikinį. Tai galite būti jūs, jei esate nuomonės formuotojas su didele auditorija, įmonės vadovas, finansų skyriaus darbuotojas ar bet kas, turintis prieigą prie vertingų duomenų ar pinigų.

Žvalgyba:

- Socialiniai tinklai: "LinkedIn" (jūsų pareigos, kolegos, profesiniai interesai), "Instagram"/"Facebook" (pomėgiai, atostogų vietos, draugai), "Twitter" (nuomonės, renginiai, kuriuose dalyvaujate).
- Įmonės svetainė: Struktūra, darbuotojų vardai, el. pašto adresų formatai.
- Tinklaidės, interviu, straipsniai: Jūsų kalbėjimo stilius, būsimi projektai, išsakytos mintys.
- Asmeninis tinklaraštis: Bet kokia papildoma informacija apie jūsų veiklą ir interesus.

Jauko Sukūrimas: Surinkę informaciją, sukčiai sukuria individualizuotą laišką ar žinutę. Jie gali paminėti jūsų kolegų vardus, projektą, ties kuriuo dirbate, konferenciją, kurioje neseniai dalyvavote, ar net hobį, kurį minėjote savo "Instagram" istorijose.

Ataka: Jums išsiunčiamas laiškas. Dėl didelio personalizacijos lygio jis neatrodo įtartinas. Jūs esate linkęs pasitikėti siuntėju ir įvykdyti prašymą – paspausti nuorodą, atidaryti dokumentą ar pervesti pinigus.

Pretexting (suklastotos situacijos kūrimas)

Įsivaizduokite, kad jums skambina žmogus, prisistatantis jūsų interneto tiekėjo techninio aptarnavimo specialistu. Jis žino jūsų vardą, adresą ir galbūt net informaciją apie paskutinį interneto sutrikimą. Jis teigia, kad atlieka būtiną tinklo patikrą ir jam reikia, kad patvirtintumėte kelis savo paskyros duomenis arba atsisiųstumėte specialią "diagnostikos" programą. Viskas skamba logiškai ir profesionaliai. Tačiau jūs kalbatės su sukčiumi.

Jautrūs duomenys

Dirbtinio intelekto mokymas

Jūsų duomenys – dirbtinio intelekto degalai

Dirbtinis intelektas (DI), ypač didieji kalbos modeliai ir vaizdų generatoriai, neveikia iš magijos. Jų veikimo pagrindas – milžiniški informacijos kiekiai, iš kurių jie “mokosi” atpažinti dėsningumus, kurti tekstą, generuoti vaizdus ir atsakinėti į klausimus. Socialiniai tinklai yra vienas didžiausių šaltinių šiems duomenims gauti. Kiekvienas jūsų įrašas, komentaras, nuotrauka ar vaizdo įrašas tampa potencialia mokymosi medžiaga.

Kodėl tai vyksta?

Technologijų gigantai kaip “Meta” (Facebook, Instagram), “Google”, “X” (buvęs Twitter) ir kiti kuria arba tobulina savo DI sistemas.

Jūsų viešai prieinamas turinys yra neįkainojamas, nes jis:

- Yra autentiškas: Tai realių žmonių sukurtas turinys, atspindintis kalbos niuansus, nuomones, humorą ir kultūrinį kontekstą.
- Yra įvairus: Milijardai nuotraukų moko DI atpažinti objektus, veidus ir situacijas. Tekstai moko kalbėti įvairiomis temomis ir stiliais.
- Yra nemokamas: Užuo mokėję už duomenų kūrimą, kompanijos tiesiog paima tai, kas jau yra viešai prieinama jų platformose.

Kokia yra rizika?

Privatumo erozija: Jūsų asmeninės istorijos, nuomonės, nuotraukos su šeima ar net pažeidžiamos mintys gali būti “įsiurbtos” į DI modelį. Vėliau tas modelis gali pateikti informaciją, paremtą jūsų patirtimi, be jokios nuorodos į jus.

Autorinių teisių pažeidimas: Menininkams, fotografams, rašytojams tai didžiulė problema. Jų unikalus darbas naudojamas apmokyti DI, kuris vėliau gali generuoti labai panašaus stiliaus kūrinius, taip nuvertindamas originalą.

Manipuliacija ir dezinformacija: Jūsų nuotraukos ar vaizdo įrašai gali būti panaudoti kuriant melagingą turinį (angl. deepfakes), taip pakenkiant jūsų reputacijai.

Kontrolės paradimas: Kartą patekę į DI modelio mokymosi duomenų bazę, jūsų duomenys ten lieka praktiškai amžinai. Jūs prarandate bet kokią kontrolę, kaip jie bus naudojami ateityje.

Svarbiausia problema: Dauguma platformų naudoja “opt-out” (atsisakymo) principą. Tai reiškia, kad jūs automatiškai sutinkate, jog jūsų duomenys būtų naudojami, nebent patys aktyviai nueisite į nustatymus ir tai uždrausite.

Fiziniai Saugumo Raktai

Tai yra aukščiausias dviejų veiksnių autentifikavimo (2FA) lygis, dar vadinamas auksiniu standartu.

Tai mažas fizinis įrenginys (panašus į USB raktą), kuris apsaugo nuo sudėtingiausių "phishing" (sukčiavimo) atakų.

Skirtingai nuo SMS ar programėlės kodų, kuriuos piktavališkas gali jus apgauti suvesti netikroje svetainėje, fizinis raktas veikia kitaip. Jis kriptografiškai patikrina, ar svetainės, prie kurios jungiatės, adresas yra tikras. Jei esate netikrame puslapyje, raktas tiesiog neveiks, taip apsaugodamas jus net jei buvote apgauti.

Jungiantis prie paskyros, po slaptažodžio įvedimo sistema paprašo įkišti raktą į USB jungtį (arba priglausti prie telefono, jei yra NFC) ir jį paliesti.



Rekomenduojami įrankiai: Yubikey

Savybės:

Tai tarsi "šveicariškas peiliukas" tarp saugumo raktų. Atsparus vandeniui, dulkėms ir smūgiams.

Palaiko daugybę autentifikavimo standartų ir turi papildomų funkcijų, pavyzdžiui, gali saugoti TOTP kodus (tuos pačius, kuriuos generuoja "Google Authenticator" programėlė).

Kam?

Pažengusiems vartotojams ir profesionalams, kuriems reikia maksimalaus lankstumo.

Kur įsigyti?

Oficialioje [Yubico](#) svetainėje arba pas platintojus Lietuvoje.

VPN

Įsivaizduokite, kad visas jūsų interneto srautas yra laiškas, keliaujantys atviruose vokuose. Kiekvienas tarpininkas nuo kavinės Wi-Fi tiekėjo iki jūsų interneto paslaugų tiekėjo (IPT) gali matyti, kam rašote ir koks yra laiško turinys.

VPN (Virtualus Privatus Tinklas) paima visus jūsų laiškus, įdeda juos į neperšaujamus, užšifruotus seifus ir išsiunčia juos šarvuotu tuneliu.

Ką VPN Daro

Šifruoja jūsų interneto srautą: Tai yra pagrindinė ir svarbiausia VPN funkcija. Visi duomenys, keliaujantys iš jūsų įrenginio, yra paverčiami neįskaitomu kodu.

Paslepia jūsų tikrąjį IP adresą: Jūsų IP adresas yra tarsi jūsų namų adresas internete, jis atskleidžia jūsų apytikslę geografinę vietą ir interneto tiekėją. VPN nukreipia jūsų srautą per vieną iš savo serverių, todėl svetainės, kurias lankote, mato VPN serverio IP adresą, o ne jūsų.

Užtikrina saugumą viešuose Wi-Fi tinkluose: Tai viena praktiškiausių VPN naudų. Prisijungę prie kavinės, oro uosto ar viešbučio Wi-Fi, su jungtu VPN galite saugiai naudotis el. bankininkyste ar jungtis prie svarbių paskyrų, nesibaimindami, kad kas nors pavogs jūsų duomenis.

Leidžia pasiekti geografiškai apribotą turinį: Kadangi galite pasirinkti serverį bet kurioje pasaulio šalyje, galite "apgauti" svetaines, kad esate toje šalyje. Taip galite žiūrėti kitų regionų "Netflix" bibliotekas, naudotis Lietuvoje blokuojamomis paslaugomis ar gauti geresnes kainas skrydžiams.

Kur įsigyti?

Įsigyti produktą galite NordVPN oficialiame tinklapyje: <https://nordvpn.com/lt/>

„NordVPN“: Išsami apžvalga

Tai lietuvių įkurtas prekės ženklas, tapęs vienu iš geriausiai žinomų ir aukščiausiai vertinamų VPN paslaugų tiekėjų pasaulyje. Remiantis naujausiomis apžvalgomis, 2025 metais "NordVPN" išlieka vienu geriausių pasirinkimų dėl greičio, saugumo ir funkcijų gausos.

Greitis: Nuolat reitinguojamas kaip vienas greičiausių VPN rinkoje, todėl puikiai tinka turinio transliacijai, žaidimams ir didelių failų siuntimui.

Saugumas ir privatumas: Siūlo ne tik standartinį šifravimą, bet ir papildomų funkcijų, tokių kaip "Threat Protection Pro", kuri blokuoja reklamas, sekiklius ir kenkėjiškas svetaines. Turi nepriklausomų auditorių patvirtintą griežtą "jokių įrašų" politiką.

Funkcionalumas: Turi didžiulį serverių tinklą visame pasaulyje, specializuotus serverius (pvz., Double VPN, P2P), patogias ir pradedantiesiems draugiškas programėles visiems įrenginiams.

Universalumas: Puikiai tinka tiek saugumui užtikrinti, tiek pramogoms (pvz., geografiškai apriboto turinio pasiekimui).