OUCH! 2024. gada

Iedomātās balsis: aizsardzība pret balss klonēšanas uzbrukumiem

Negaidītais zvans: stāsts par maldināšanu

Mārgareta, pensionēta skolotāja, izbaudīja mierīgu rītu savā nelielajā piepilsētas mājā. Kādu dienu, baudot rīta kafiju, viņa saņēma satrauktu zvanu no sava mazdēla Džeikoba, kurš bija devies uz universitāti. Viņa balsī bija jūtama panika, viņš paskaidroja, ka ir iekļuvis autoavārijā un steidzami esot vajadzīga nauda, lai samaksātu par zaudējumiem un izvairītos no juridiskām problēmām. Ja viņš naudu nesaņems uzreiz, viņš varot nonākt cietumā. Balss otrā galā nepārprotami piederēja Džeikobam – Mārgaretai no satraukuma sažņaudzās sirds. Nešauboties viņa steidzās uz banku un pārskaitīja naudu uz Džeikoba norādīto kontu. Tikai vēlāk tajā pašā dienā, kad Mārgareta piezvanīja Džeikoba mātei, lai uzzinātu, kā Džeikobam klājas, viņa uzzināja, ka ir apkrāpta. Zvans bija ļauns triks, kibernoziedznieks izmantoja mākslīgā intelekta (MI) balss klonēšanas tehnoloģiju, lai atdarinātu Džeikoba balsi, tādējādi ļaunprātīgi izmantojot Mārgaretas mīlestību un rūpes par mazdēlu.

Kas ir balss klonēšana?

Balss klonēšana tiek veikta, izmantojot mākslīgo intelektu, lai atveidotu cilvēka balsi, iekļaujot balss īpatnības, intonāciju un runas ritmu, tādējādi radot gandrīz perfektu kopiju.

Balss klonēšanas uzbrukums sākas ar to, ka kibernoziedznieks ievāc mērķa balss audio paraugus. Šos paraugus var iegūt no dažādiem avotiem, piemēram, videoklipiem vietnē YouTube vai personīgiem ierakstiem vietnē TikTok. Pēc ierakstītā audioieraksta apstrādes mākslīgais intelekts ģenerē jaunu audioierakstu, kas izklausās līdzīgi ieraksta mērķa audio paraugam. Šo ģenerēto balsi var izmantot dažādos veidos, sākot ar tālruņa zvaniem un beidzot ar balss ziņojumiem, tādējādi padarot to par spēcīgu krāpšanas rīku.

Sagatavojot balss klonēšanas uzbrukumus, kiberuzbrucēji bieži vien vispirms veic izpēti. Lielākā daļa viņiem nepieciešamās informācijas ir publiski pieejama sociālo mediju vietnēs. Viņi izpēta savus iecerētos upurus, lai iekļautu gan personas balsi, kuru viņi gatavojas replicēt, gan arī upuri, kuram viņi gatavojas zvanīt. Kibernoziedznieki ne tikai uzzina, ko viņu upuri pazīst un kam uzticas, bet arī to, kuri emocionālie ierosinātāji ir visefektīvākie. Veicot šādus tālruņa zvanus, kiberuzbrucēji bieži vien maina zvanītāja identifikāciju , lai, upurim paskatoties tālrunī, šķistu, ka zvans nāk no uzticama numura. Zvanītāja identifikāciju var viegli viltot, un tas nav labs veids, kā apstiprināt vai autentificēt cilvēkus, kas jums zvana.

Aizsargāt sevi

Pirmais solis, lai sevi aizsargātu, ir vienkārši apzināties, ka balss klonēšana tagad ir iespējama un kiberuzbrucējiem kļūst arvien vieglāk to paveikt. Dažas svarīgākās lietas, ko vajadzētu ņemt vērā:

- **Privātums**: Apzinieties un ierobežojiet informāciju, ar kuru dalāties ar citiem, un ierobežojiet to, kas var piekļūt jūsu ierakstiem sociālajos tīklos.

- **Norādes**: Uzmanīgi sekojiet līdzi ierastajiem signāliem, kas liecina par to, ka kaut kas nav kārtībā. Ja kāds jums zvana un rada lielu steidzamības sajūtu vai piespiež nekavējoties rīkoties, visticamāk, tā ir krāpšana. Jo lielāka steidzamības sajūta tiek radīta, piemēram, pieprasot naudu uzreiz, jo lielāka iespēja, ka kāds cenšas jūs piespiest kļūdīties. Citi bieži sastopami signāli ir arī tādi, kad ir sajūta, ka kaut kas ir pārāk labs, lai tā būtu patiesība (nē, jūs nelaimējāt loterijā, kurā nepiedalījāties), vai kad saņēmāt negaidītu zvanu, kas šķita dīvains.

- **Pārbaude**: Ja neesat pārliecināts, ka zvans ir patiess, nolieciet klausuli un pārzvaniet uz uzticamu numuru. Piemēram, ja jums zvana kāds uzņēmuma augstākā līmeņa vadītājs vai kolēģis, pārzvaniet uz jums zināmu konkrētā uzņēmuma/kolēģa patieso numuru. Ja saņemat neparastu zvanu no ģimenes locekļa, mēģiniet viņam piezvanīt atpakaļ (iespējams, pat izmantojiet videozvanu) vai zvaniet citam konkrētā tuvinieka ģimenes loceklim.

- **Parole**: Izveidojiet slepenu frāzi vai paroli, ko zināt tikai jūs un jūsu ģimene. Šādā veidā, ja saņemat neparastu zvanu, ko, iespējams, veic kāds ģimenes loceklis, varat pārbaudīt, vai tas patiešām ir viņš/viņa, pajautājot, vai viņš/viņa zina jūsu slepeno paroli.

Viesredaktors

Marija Singa (Maria Singh) ir EnterpriseKC kibersatursatura vadītāja un kaislīga WiCyS dalībniece ar vairāk nekā 14 gadu pieredzi tehnoloģiju un kiberdrošības jomā. Viņai ir SANS GIAC GSEC sertifikāts un viņa ir Perdjū Universitātes kiberdrošības maģistra grāda kandidāte. Būdama Women in Security Kansas City bijusī prezidente un OCA Corporate Achievement balvas saņēmēja, Marija iedvesmo sievietes STEM un kiberdrošības jomā. Viņas uzstāšanās un vadošā loma bruģē pamatu nākamajām paaudzēm uzplaukt šajās jomās.

Resursi

Trīs izplatītākie veidi, kā kiberuzbrucēji vēršas pret jums: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Pārtraukt tālruņa zvanu krāpšanu: https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Emocionālie ierosinātāji – kā kiberuzbrucēji piemāna cilvēkus: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Tulkojums: CERT.LV