OUCH! Mart 2022

Zaštitite se od prevare - prepoznajte dipfejk

Šta je to dipfejk?

Naziv dipfejk (eng. "deepfake", bukvalni prevod: duboki falsifikat) je izvedenica od pojmova “deep learning” (fenomen koji opisuje sposobnost računara da izvode zaključke i uče na osnovu analize podataka) i “fake” (lažno). Dipfejk su lažne (falsifikovane) fotografije, video snimci ili audio zapisi. Ponekad se u njima pojavljuju ljudi koji ne postoje već se radi o kompjuterski generisanim lažnim identitetima koji izgledaju i zvuče kao da su stvarni. U drugim slučajevima pojavljuju se ljudi koji su stvarni, ali se njihovim prikazom i glasovima manipuliše na način da rade ili govore nešto što nisu uradili ili rekli. Na primer, dipfejk video se može upotrebiti tako da se korišćenjem lika neke poznate ličnosti ili političara lažno prikaže da je taj neko nešto rekao. Na taj način, napadači mogu da stvore privid stvarnosti i da nas dovedu u situacije u kojima ne možemo verovati sopstvenim očima i ušima.

Neki dipfejkovi mogu imati i legitimne svrhe, poput filmova koji vraćaju u život preminule glumce, kako bi se ponovo oživeo poznati lik. Međutim, u poslednje vreme sajber kriminalci počinju da iskorišćavaju pun potencijal dipfejk prevara. Oni ih koriste da zavaraju vaša čula, kako bi vam ukrali novac, uznemiravali ljude, manipulisali biračima ili političkim stavovima, ili kreirali lažne vesti. Zabeleženi su čak i slučajevi kreiranja lažnih kompanija koje imaju samo dipfejk zaposlene. To znači da treba da još više da pazite u šta ćete da poverujete kada se informišete putem vesti ili društvenih mreža.

FBI upozorava da će dipfejk u budućnosti imati „još ozbiljniji i rasprostranjeniji uticaj zbog nivoa sofisticiranosti sintetičkih medija koji se koriste za njihov kreiranje“. Zbog toga je potrebno da se pripremite - naučite kako da prepoznate dipfejk da biste se zaštitili od ovih veoma uverljivih simulacija. Svaki oblik dipfejka — zamrznuta slika, video i audio zapis — ima sopstveni skup nedostataka koji ga mogu odati.

Zamrznute slike

Dipfejk sa kojim se verovatno najčešće susrećete je lažna slika profila na društvenim mrežama. Slika u nastavku teksta predstavlja jedan primer dipfejka sa veb sajta thispersondoesnotexist.com. Ispod slike je navedeno pet različitih znakova koji ukazuju da se ovde radi o dipfejku. Primetićete da ove tragove nije lako uočiti:

1. Pozadina: Pozadina je često mutna ili iskrivljena i može biti različito osvetljena - npr. izražene senke se mogu pružati u različitim pravcima.
2. Naočare: Pažljivo pogledajte spoj između okvira i drški u blizini slepoočnice. Dipfejk često ima neujednačene prelaze između različitih veličina ili oblika.
3. Oči: Kod dipfejk fotografija koje se koriste kao profilne fotografije oči često izgledaju kao da se nalaze u istom položaju u kadru, što za rezultat ima takozvani "dipfejk pogled".
4. Nakit: Minđuše mogu biti bezoblične ili neobično pričvršćene. Ogrlice mogu biti ugrađene u kožu.
5. Kragne i ramena: Ramena mogu biti deformisana ili neodgovarajuća. Kragna sa jedne i druge strane se može razlikovati.

Video

Istraživači sa Tehnološkog instituta u Masačusetsu, MIT, osmislili su listu pitanja koja vam može pomoći da shvatite da li je video stvaran, napominjući da dipfejk često ne može „u potpunosti da predstavi prirodnu fiziku“ scene ili osvetljenja.

1. Obrazi i čelo: Da li koža deluje previše glatko ili previše naborano? Da li starost kože odgovara starosti kose i očiju?
2. Oči i obrve: Da li se senke pojavljuju na mestima na kojima ih očekujete?
3. Naočare: Ima li odsjaja? Da li ga ima previše? Menja li se pozicija odsjaja kada se osoba pomera?
4. Malje na licu: Da li malje na licu izgledaju prirodno? Dipfejk može da doda ili ukloni brkove, zulufe ili bradu.
5. Mladeži: Da li mladež izgleda kao da je pravi?
6. Treptanje: Da li osoba trepće uobičajeno ili prečesto?
7. Veličina i boja usana: Odgovaraju li veličina i boja usana ostatku lica?

Audio/glas

Istraživači tvrde da tehnologije poput spektrograma mogu da ukažu da su glasovni zapisi lažni. Međutim, većini od nas nije u prilici da koristi analizator glasa kada nas kriminalac pozove. Obratite zato pažnju na monotonost glasa, čudne zvuke ili emocije, kao i na izostanak pozadinske buke. Lažiran glas može biti veoma teško uočiti. Ako primite neobičan poziv od legitimne organizacije, možete proveriti da li je poziv stvaran tako što ćete prekinuti vezu, a zatim ponovo nazvati tu organizaciju. Pritom obavezno koristite pouzdan telefonski broj organizacije, kao što je broj telefona koji već imate na listi kontakata, broj telefona odštampan na računu ili nekoj potvrdi koju ste od organizacije dobili ili broj telefona objavljen na zvaničnom sajtu organizacije.

Zaključak

Imajte na umu da kriminalci aktivno koriste dipfejk. Oni mogu napraviti lažne naloge na društvenim mrežama koje će koristiti za povezivanje sa drugima ili kreirati lažne video zapise kako bi uticali na javno mnjenje. Neki od njih čak prodaju svoje usluge na dark vebu, nudeći ih drugim kriminalcima na korišćenje. Ne očekuje se od vas da postanete stručnjak za dipfejk, ali ako savladate osnove za njegovo prepoznavanje, bićete daleko uspešniji u svojoj odbrani. Ako posumnjate da ste otkrili dipfejk, prijavite to vebsajtu ili izvoru koji hostuje taj sadržaj.

Gost urednik

Keri Tomlinson (@KerryTNews) je izveštač za sajber vesti u Ampere News-u i sertifikovani profesionalac SANS instituta u domenu unapređenja svesti o sajber bezbednosti. Njena misija je da približi dešavanja u digitalnom svetu ljudima svih nivoa znanja korišćenjem zanimljivih, njima prilagođenih vesti i prezentacija.

Dodatni materijal

Socijalni inženjering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Can you spot the fake? (Ampere News): https://www.amperesec.com/news/can-you-spot-the-fake
MIT's deepfake detection test (MIT): https://detectfakes.media.mit.edu/
Spot the deepfake: https://www.spotdeepfakes.org/en-US

Preveli za zajednicu: Dragan Ristić i Gordana Živanović:
 Redakcija: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.