DEEPFAKE, YANGI NFS QURILMALARI VA SKIMMING KIBERJINOYATLARI.

Yusupov Faxriddin Hurmatboy o‘g‘li
O‘zbekiston Respublikasi Ichki Ishlar Vazirligi Akdemiyasi kursanti

Annotatsiya: *Ushbu maqola orqali siz, O‘zbekistondagi kiberjinoyatlarning yangi to‘lqini sifatida gavdalanayotgan DeepFake, yangi NFS qurilmalari, Skimming kabi kiberhuquqbuzarliklar tushunchasi, sodir etilish usullari, turlari, jabrlanuvchilar tomonidan yo’l qo’yilayotgan xatolar va ulardan himoyalanish chora-tadbirlari haqida batafsil ma’lumotga ega bo‘lishingiz mumkin.*

Kalit so‘zlar: *Face2Face, Deepface, kollabaratsiya, manipulyatsiya, skimming, integratsiya, HMQO, sxema, chip.*

Annotation: *Through this article, you will learn in detail about the concept of cybercrimes such as DeepFake, new NFS devices, Skimming, which are being embodied as a new wave of cybercrimes in Uzbekistan, methods of committing, types, mistakes made by victims and measures to protect against them. you can have information.*

Keywords: *Face2Face, Deepface, collaboration, manipulation, skimming, integration, HMQO (LEA) , scheme, chip.*

Аннотация: *Из этой статьи вы подробно узнаете о концепции таких киберпреступлений, как DeepFake, новых устройствах NFS, Skimming, которые воплощаются в виде новой волны киберпреступлений в Узбекистане, способах их совершения, видах, ошибках, допущенных жертвами, и мерах по их предотвращению. защититься от них.Вы можете иметь информацию.*

Ключевые слова: *Face2Face, Deepface, сотрудничество, манипуляция, скимминг, интеграция, HMQO (ПОО) , схема, чип.*

DEEPFAKE

Deepfake – soxta kontent yaratish maqsadida, insonni yuz qiyofasi, ovozi, harakati, jesti va boshqa xususiyatlarini sintetik vositalar yordamida ishonchli tarzda o‘xshatish uchun raqamli manipulyatsiyalashdir[17].

Ushbu so‘zni lug‘aviy jihatdan tarjima qilinganda “chuqur soxtalashtirish” ma’nosini keltirib chiqaradi. Aslida tarixan olib qaraydigan bo‘lsak, Deepfake so‘zi 2017-yilda kirib

[17] https://en.m.wikipedia.org/wiki/Deepfake

kelgan bo‘lib, ungacha ushbu texnologiyalar Face2Face, Deepface nomlari bilan atalgan.[18] Deepfake texnologiyalari 1997-yilda Kristofer Bregler, Mishel Kovell va Malkolm Slaneylar tomonidan ishlab chiqilgan bo‘lib, ular inson yuzidagi ba’zi bir nuqtalarni o‘zgartirish xususiyatini ixtiro qilishgan.[19] Keyinchalik ushbu texnologiyalar ovoz va boshqa xususiyatlarni ham o‘z ichiga qamrab olganligi sababli, nomi Deepfake ga o‘zgargan. Endi ushbu texnologiyalar qanday qilib huquqbuzarlik holatlarini keltirib chiqarish mumkinligini ko‘rib chiqsak.


O‘zbekistonda Deepfake huquqbuzarliklari asosan 2 xil usul bilan, ya’ni ovoz va yuz tuzilishini o‘zgartirish orqali sodir etilmoqda. Avvallari, Deepfake programmalar va saytlar orqali amalga oshirilgan bo‘lsa, hozirda sun’iy intellekt rivojlanib ketganligi sababli, birgina rasm va qisqa soniyali ovoz tonlari orqali xohlagan insonning video, gif, foto va audio fayllarini yaratish mumkin. Huquqbuzarlar ham aynan shular orqali, ya’nikim mashxur shaxslar, tadbirkorlar, artistlar yoki davlat hokimiyati rahbarlarining yuz hamda ovozlaridan foydalanib firibgarlik va boshqa jinoyatlarni sodir etishmoqda. Ularning ko‘pchiligini asosiy mavzusi o‘xshash, to‘g‘rirog‘i noqonuniy hisoblangan moliya piramidalari, birjalar, treyding xizmatlari yokida erkin savdosi taqiqlangan maxsulotlar (narkotik va psixotrop moddalar, pnevmatik qurollar va boshqalar)ni shaxsan tavsiya qilish.

Hozirda quyidagi saytlar orqali deepfakeni yasashda yuqori sifatga erishish mumkin.

- Voice.ai
- Descript.com
- iSpeech.com
- Fakeyou.com
- Voice.headliner.app
- Deepswap
- Faceswapper.ai
- Swapface.org
- FaceHub

Yuqorida keltirilgan saytlar sun’iy intellekt bilan kollabaratsiyalashib, ovoz va yuz qiyofasini ancha yuqori sifat bilan integratsiyalashtiradi. (Eslatib o‘tamiz fuqarolarning shaxsiy xususiyatlaridan ularning ruxsatisiz foyalanish qonunga ziddir. Shu sababdan yuqorida sanab o‘tilgan vebsaytlardan ba’zilari SPAM olganliklari tufayli, hozirda faoliyat olib bormayotgan bo‘lishi mumkin.) Ularning aksariyati pullik xizmat ko‘rsatadi. Pullik

[18] https://baasith-shiyam1.medium.com/deepfakes-and-their-history-e6d926ae56cf
[19] https://networthpick.com/2021/06/05/demystified-the-24-year-history-of-deepfakes-and-the-fight-back-against-them/

xizmatlar orqali, tekin rejimga qaraganda, ancha yuqori sifatga va qo‘shimcha imkoniyatlarga erishish mumkin.

Yangi NFS qurilmalari

Yangi turdagi NFS qurilmalari haqida gapirishdan avval, NFSning o‘zi qanday ishlashi haqida to‘xtalib o‘tsak. NFS plastik kartalardan tashqari ko‘pgina qurilmalarga o‘rnatilgan bo‘lib, uni bajaradigan asosiy vazifasi uncha katta bo‘lmagan ma’lumotlarni bir qurilmadan boshqasiga uzatishdan iborat. Hozirda ishlayotgan plastik kartalarga mikro chiplar o‘rnatilgan bo‘lib, ular juda qisqa vaqt ichida, ma’lum bir chastotalarga javob qaytaradi. Shu qisqa fursatdagi so‘rov va javob ichida quyidagilar amalga oshadi. Dastavval qurilmadan ushbu plastikdan qancha miqdordagi pul yechish, plastik kodini yokida raqamini almashtirish, sms xabarnomani o‘chirib-yoqish kabi bir qancha amallarni bajarish uchun so‘rov yuboriladi. NFS texnologiyasi mavjud bo‘lgan plastik kartalarda, yuqoridagi barcha amallarni bajarilishi, faqatgina plastik karta kodi orqali amalga oshiriladi. Ba’zi holatlarda bu harakatlarni bajarilishi kodsiz ham amalga oshishi mumkin. Masalan HUMO plastik kartasidan 50000 (ellik ming) so‘mgacha pul miqdorini NFS orqali kodsiz yechib olishingiz mumkin. Bu aslida foydalanuvchilarga qulaylik yaratish uchun, ya’ni ortiqcha ovoragarchiliklarni yo‘qotish maqsadida yaratilgan.

Biroq shu kabi imkoniyatlardan g‘arazli yo‘llarda ham foydalanish mumkin. Aniqroq qilib aytganda, plastik kartalardan NFS yordamida faqatgina 50000 so‘mgacha bo‘lgan pul miqdorini yechish kerakligini o‘sha qurilmaga buyruq qilib berish orqali. Buni sizga bir qurilma orqali batafsil tushuntirib bersak.

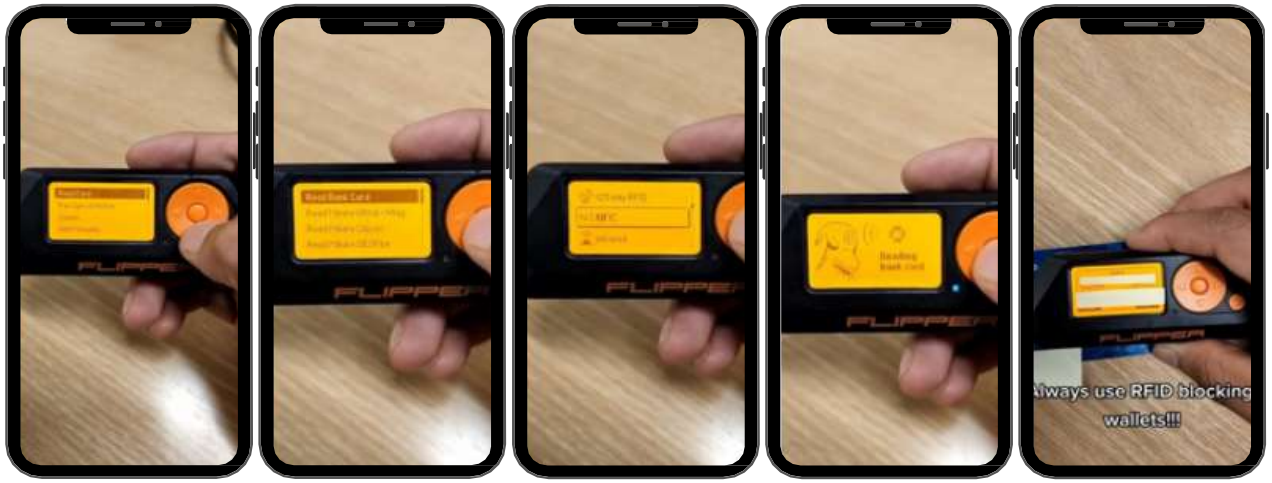
Quyida tasvirlangan Flipper Zero yuqorida sanab o‘tilgan vazifalarni bajarishda yuqori koeffisentga ega.

Ushbu qurilmada plastik kartalarni skaynerlashdan tashqari boshqa ko‘pgina imkoniyatlar mavjud.

Ular quyidagilar:

- Plastikka birgina tegish orqali, plastik karta va uning egasi haqida ma’lumotlarga ega bo‘lish;
- Plastik kodi yoki raqamini o‘zgartirish;
- SMS xabarnomani yoqishi yokida o‘chirib qo‘yish;

- Plastik karta ichida qancha pul mablag‘lari borligini bilish, uni NFS orqali belgilangan miqdorda hech qanday kodsiz yechib olish va hokazolarni amalga oshirish mumkin.



Va nihoyat jamoat joylari va transport vositalarida yoki bo‘lmasa, siz e’tibor bermagan holatlarda, huquqbuzar sizning plastik kartangizga birgina tegish orqali ma’lum miqdordagi mablag‘larni yechib oladi. Bu mablag‘lar sizga kichik summa bo‘lib ko‘rinishi mumkin, lekin huquqbuzar faqat sizning kartangizdagi pullarni yechish bilan cheklanib qolmaydi. U yuqoridagi harakatlarni yuzlab, minglab, hatto yuz minglab fuqarolar bilan ham amalga oshirishi mumkin. Juda kichik bo‘lib tuyulgan bu mablag‘lar, yig‘ilib-yig‘ilib millionlab summani tashkil etadi. Bu esa uni davomli jinoyat sifatida ijtimoiy xavflilik darajasini yanada oshiradi.

Shu sababli ushbu turdagi huquqbuzarliklar hamon o‘z dolzarbligini saqlab qolmoqda.

SKIMMING

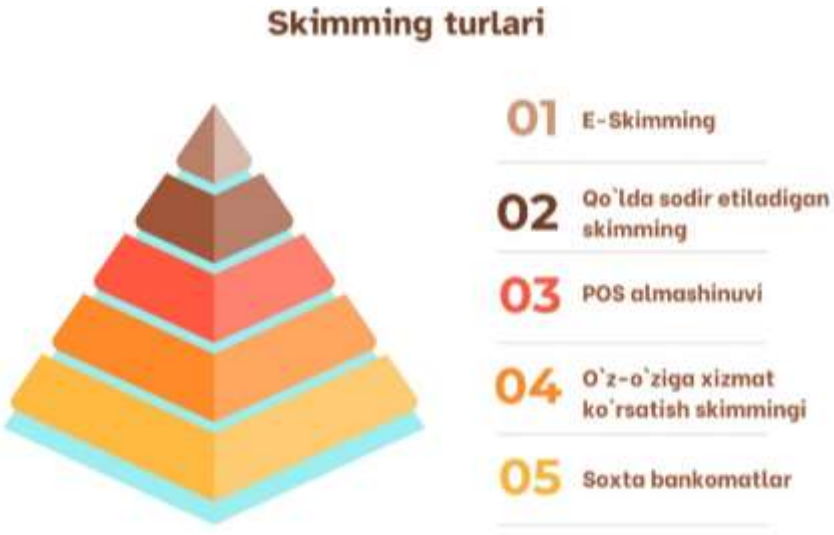
Skimming – bu bank karta ma’lumotlarini noqonuniy qo‘lga kiritishdan iborat bo‘lgan kiberjinoyat turi hisoblanadi. Uning sodir etilish joylari asosan bankomatlar, terminallar va savdo shaohbchalari atrofida kichadi.

Skimming - so‘ngi yillar ichida yurtimizda rivojlanib borayotgan, shu bilan birga ushbu huquqbuzarlarni shaxsiga aniqlik kiritish borasida bir qancha murakkabli vaziyatlarni keltirib chiqayotganligi sababli, kiberjinoyatchilar orasida keng tarqalmoqda.

Bu turdagi huquqbuzarlik ham yurtimizda asosan 2 ko‘rinishda sodir etilmoqda. Ular:

1. Bankomatning qismlariga o‘zining qo‘shimcha uskunalarini o‘rnatish orqali;

2. Plastikka o‘xshash mikrosxema yasab, unga, o‘zidan keyin kirgan plastikni, o‘zining dasturiga kirib ketishni ta’minlovchi kod yozish orqali.



Bankomatning qismlariga o‘rnatilayotgan uskunalar, asosan bankomatning quyidagi joylariga o‘rnatilmoqda.

- Bankomatning plastik kiritish kanali (halqasi) atrofiga. Bu qismiga qo‘yilishidan asosiy maqsad plastigingizning raqami, amal qilish muddati, qaysi bankka tegishli ekanligi, to‘lov tizimini (HUMO, Uzcard, Mastercard, VISA va hokazo) bilishdan iborat. Plastik kiritish kanaliga ko‘p holatlarda makro-obyektivkali kameralar o‘rnatiladi, ya’ni yaqin masofada kirayotgan plastik ma’lumotlarini o‘qish maqsadida.
- Keyingi nuqta esa bankomatning raqamlar joylashgan klaviaturasi (klavishi, tugmalari). U yerga qo‘yilishidan birdan bir maqsadi, kartangizning kodlarini bilib olishdir. Bu tugmalarga siz tergan raqamlarni ketma-ketlik kombinatsiyasini eslab qoluvchi chiplar o‘rnatiladi

Ikkinchi ko‘rinishi haqida gaplashadigan bo‘lsak. Bu huquqbuzarlikda kiberjinoyatchi plastik kartaga o‘xshash sxema (chip) yasaydi va unda plastik kartada bo‘ladigan barcha datchiklarni joylashtiradi. Shuningdek unga maxsus kod ham yozadi. Bu kod 2 xil vazifani bajarish uchun mo‘njallanadi.

Birinchisi, bankomatga yuqoridagi kabi maxsus tayyorlangan plastik karta kirganidan so‘ng, shu plastik kartadan keyin kiradigan birinchi plastikni o‘zi tuzgan dasturga kirgazib

yuborish. Ya'ni fuqaro bankomatning tizimiga emas, kiberjinoyatchi yozgan dasturga kirib ketadi va ko'p holatlarda u o'ljaga aylanadi.

Ikkinchisida esa, plastik kartaga yozilgan maxsus dastur - fuqarolar uchun emas, balki bankomatning tizimini buzish uchun tuzilgan bo'ladi. Buni oddiy qilib tushuntirganda, barcha fuqarolarning bank kartasi ma'lumotlari, ularning plastik kartasi raqamlari bilan belgilangan ma'lumotlar omborida saqlanadi va unga kirish faqatgina kod orqali amalga oshadi. Bankomat esa, shaxs kiritgan plastik karta raqami va kodi orqali o'sha manbadagi hisobni ochadi. Kiberjinoyatchi esa o'sha manbada hisob o'rniga maxsus dastur yozib qo'ygan bo'ladi yoki boshqacha usullar bilan huquqbuzarlikni sodir etadi.

Ikkinchi ko'rinishdagi kiberhuquqbuzarlikni faqatgina maxsus bilimga ega bo'lgan shaxslar sodir etadi. Shu sababli, bu turdagi kiberjinoyatlarning sodir etilish salmog'i boshqalariga qaraganda ancha past. Zamon rivojlanib borgani sayin, yuqoridagi kabi kiberhquqbuzarliklarning turlari va sodir etish usullari tadrijiy rivoj topib bormoqda.

Sodir etilish sabablari

Muhokama etilayotgan 3 turdagi kiberhuquqbuzarlikning sodir etilish salmog'i oshishi va aniqlash imkoniyati pastligining eng asosiy sababi bu – sodir etayotganlarning shaxsini aniqlash imkoniyati kamligi. Aynan shu sabab, texnik bilimga ega bo'lmagan, oddiy fuqarolar tomonidan ham sodir etilish holatlari oshmoqda. Negaki jinoyat izlari, dalillar, guvohlar va jinoyat ochishda yordam beradigan tusmollar – an'anaviy turdagi huquqbuzarliklar bilan solishtirganda deyarli yo'q hisob.

Shu bilan birga yuqoridagi huquqbuzarliklarning latentlik darajasi yuqoriligi (obyektiv va subyektiv omillarga ko'ra, huquqni muhofaza qiluvchi organlarga (keyingi o'rinlarda HMQO deb yuritiladi) murojaat qilmaslik), o'zlarining ehtiyotsizligi tufayli sodir etilganligi bois, huquqbuzarga javobgarlik yo'q deb o'ylashi, yetkazilgan ziyonni kamligi sababli yoki HMQOlariga ishonchsizligi va hokazolar sabab bo'lmoqda.

Profilaktika

Ushbu turdagi huquqbuzarliklardan saqlanish maqsadida quyida keltiriladigan profilaktik chora-tadbirlarni, kundalik faoliyatingizga kiritishingizni so'rab qolamiz:

- ijtimoiy tarmoqlarga shaxsiy video, fotosuratlar va ma'lumotlarni joylashtirmang;
- maxfiylik sozlamalariga amal qiling, xavfsizlik siyosatini to'g'ri yuriting va begona shaxslar uchun profilingizni yoping;
- plastik kartalaringizni qattiq g'iloflarda va kiyimingingizning ichki qismlarida saqlang;
- bankomatdan foydalanishdan oldin, uni yaxshilab tekshirib ko'ring (plastik kiritish kanali, klavishi va yuqori qismida kamera yo'qligiga) va kodni terishda hech kim qaramayotganligiga e'tibor bering;
- yuqorida eslatib o'tilgan, ya'ni firibgarlar o'zining uskunalarini qo'yishi mumkin bo'lgan joylarni ehtiyotkorlik bilan tekshirib chiqing;
- bankomatni ishlatishda iloji boricha NFSdan foydalaning.
- imkon qadar do'kon, bozor, savdo shahobchalarida to'lovni naqd pul orqali yoki telefoningdan (yoxud NFS bilan) onlayn tarzda o'tkazing.

Xususan, birinchi navbatda shaxsiy xavfsizlik va texnik qoidalariga to‘liq rioya qilishingiz, faqat ushbu turdagi huquqbuzarliklar emas, balki boshqa har qanday ko‘rinishdagi kiberjinoyatlarning jabrlanuvchisiga aylanishingizni oldini oladi.

Xulosa o‘rnida shuni ta’kidlab o‘tish joizki, zamon shiddat bilan o‘zgarib borgani sari, undagi ijtimoiy hayot yo‘nalishlari ham rivojlanib boradi. Ya’ni texnik, dasturiy va kommunikatsion ixtiro, innovatsiya va yangiliklar bilan birga, nur va soya kabi uning teskari tomoni ham tom ma’noda taraqqiy etib boradi. Ya’nikim, kun sayin paydo bo‘layotgan yangi kiberjinoyatlarning har biriga alohida va individual profilkatik chora-tadbirlar ishlab chiqish va uni ommaga tatbiq etish uchun vaqt cheklangan. Shu sababli aholi o‘rtasida texnik madaniyatni oshirish va ijtimoiy profilaktik choralarni keng tatbiq etish, kiberjinoyatlarni oldini olish va qarshi kurashish borasidagi eng muqobil tanlovdir.

FOYDALANILGAN ADABIYOTLAR:

1. DeepFakes. Creation, Detection, and Impact
1. https://en.wikipedia.org/wiki/Deepfake
2. Brief Summary of Book: Deepfake by Sarah Darer Littman
4. https://en.m.wikipedia.org/wiki/Deepfake
5. https://baasith-shiyam1.medium.com/deepfakes-and-their-history-e6d926ae56cf
6. https://networthpick.com/2021/06/05/demystified-the-24-year-history-of-deepfakes-and-the-fight-back-against-them/