



VIRTUAL OLAMDAGI JINOYATLAR

Jalilova Muhayyo

*Andijon davlat universiteti ijtimoiy-iqtisodiyot
fakultteti Amaliy psixalogiya yo 'nalishi talabasi*

Annotatsiya: Ushbu maqola "Virtual olamda keng tarqalgan jinoyatlardan biri bu Plastikkarta foydalanuvchilarining hisoblaridan pul o'g'irlashdir" degan mavzuga bag'ishlangan xavfsizlik muammolarini o'z ichiga oladi. Firibgarlik, kiber jinoyatchilik, va zararli viruslar kabi virtual olamning eng muhim muammolari ko'rsatkichi bo'lib, ularga qarshi kurashish juda muhimdir. Bu maqolada, Plastikkarta orqali amalga oshiriladigan "Fishing" deb nomlangan firibgarlik usulini, onlayn savdodagi firibgarliklar, va zararli viruslar haqida ma'lumot berilgan. Aynan shu sababli, virtual olamda xavfsizlikni ta'minlashga e'tibor berish zarur. Virtual olamdagi jinoyatlar, kiberxavfsizlikning muammosi, va kiberjinoyatlar statistik ma'lumotlari haqida maqola ko'rsatkichi, virtual olamda xavfsizlikni ta'minlashning muhimligi, va virtual olamdan o'z xavfsizligimizni himoya qilishning zarurati qayd etilgan. Maqoladagi statistik ma'lumotlar, virtual olamdagi jinoyatchilikka qarshi kurashishning muhimligini ta'kidlaydi. Virtual olamda xavfsizlikni ta'minlash uchun ijtimoiy tarmoqdagi xabarlar va notanish kimsalarga ishonib qolish, virtual olamdan real hayotga ajratib qolish, va jinoyatlar tuzog'iga tushmagan holda faol bo'lish, kiberxavfsizlikni ta'minlash uchun keng imkoniyatlarni yaratadi.

Kalit so'zlar: Virtual firibgarlik, kiberjinoyatlar, virtual tahdidlar, internet, bank kartalari,, axborot xurujlari, onlayn savdo maydonidagi firibgarliklar, kiberxavfsizlik.

Hozirgi zamonaviy kommunikatsiya bilan qurilgan dunyoda hayotimizni o'tkazishimizda zamonaviy rivojlanishga tufayli qulayliklar paydo bo'ldi. Axborot kommunikatsiyasining bugungi kunda qo'shilayotgan xissasi beqiyos hisoblanadi. Virtual olam orqali amalga oshirishimizni qulaylashdi. Axborot sohasidagi globalizatsiya ko'rsatkichi qanchalik yuqori cho'qqiga chiqmoqda, millionlab yoshlar internet tarmoqlarida keng foydalanib, mablag' ishlab topish orqali o'zlariga kerakli va zarur bilimlarni o'zlashtirishmoqda. Hozirgi kunda virtual olamsiz hayotimizni tasavvur qilish qiyin bo'lgan hodisa hisoblanadi. Virtual olam hayotimizga yengiliklar keltirish bilan birga unga tahdid ham solmoqda, lekin bu tahdidlarga qarshi ko'z yumishning esa sira iloji yo'q. Bunday tahdidlarning asosiy manbai internet tarmogi hisoblanadi. Internet dunyosidagi kashfiyotlar tufayli hayotimizda qulayliklar va imkoniyatlar paydo bo'ldi, lekin bu qulayliklar va imkoniyatlar kiber jinoyatlar deb nom olgan sohaning rivojlanishiga ham o'z xissasini qo'shib kelmoqda. "Kiber jinoyatchilik" tushunchasi axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda virtual tarmoqda jinoyat sodir etish, virus va boshqa zararli dasturlarni tarqatish, xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik ma'lumotlarini va mualliflik huquqini buzish, kredit kartochkalari raqami va bank rekvizitlarini o'g'irlash, o'zgaruvchilar hisob raqamlariga mablag'ni o'g'irlash, boshqalar nomidan jinoyatlar sodir etish va boshqa ko'plab usullar orqali huquqbuzarliklar qilish va jinoyat sodir etish kabi holatlar tushuniladi.

Hozirgi kunda virtual olamda keng tarqalgan firibgarliklardan biri bu Plastikkarta foydalanuvchilarining hisoblaridan pul o'g'irlashdir. Respublikamizda so'ngi



paytlarda UZCARD tizimidagi plastik kartalaridan pul o'g'irlash holatlarining ko'pchayotganini ko'zatisish mumkin. Bunday virtual firibgarlik "Fishing" deb nomlanadi. "Fishing" ya'ni "baliq ovi" usulidir. Bunda IT texnologiyasi sohasida yetarlibilim va tajribaga ega firibgarlar tomonidan bank kartasidan foydalanuvchilarningishonchiga kirib bank kartasiga doir maxfiy ma'lumoylarni egallash tushuniladi. Shu o'rinda firibgarlar bu ishlarni qanday amalga oshirmoqda degan savol tug'iladi. Busavolga esa quydagicha javob berish mumkin; plastik kartada savdo qilish, xizmatko'rsatish, kommunal va boshqa to'lovlarni amalga oshirish biz uchun anchaqulay. Lekin bu kabi operatsiyalarni amalga oshirishda SMS orqali keladigan maxfiy kodni boshqalarga berish yoki plastik kartadagi 4 ta raqamdan iborat maxfiy kodlarni boshqalarga aytish xatarli hisoblanadi. Afsuski, firibgarlar odamlarningishonuvchanligidan foydalangan holda, o'zini bankdan, Click, Payme yoki boshqa to'lov xizmatlari tashkiloti xodimi ekanini aytib fuqarolarni aldab, ushbu ma'lumotlarni so'raganda, plastik karta egalari bu ma'lumotlarni berib yuborish holatlari ko'pkuzatilmoqda. Firibgarlar mana shunday vaziyatlardan foydalanib odamlarning plastik kartalaridan pullarini yechib olib ularga juda katta molyaviy zararlarni yetkazmoqda. Firibgarlarning tuzog'iga tushib qolmaslik uchun; shaxsiy bank kartalaridagi parol va kodlaringizni hech kimga aytmang yoki bermang. Kartabo'yicha SMS ogohlantirish xizmatini ulang. Xavfsiz saytlarni tanlang. Shundagina firibgarlar tuzog'iga tushib qolish ehtimolingiz ancha kamayadi. Virtual olamdagi yanakeng tarqalgan jinoyatlardan biri bu diniy aqidaparastlikka qaratilgan o'zidaterrorchilik va terorizm g'oyalarini targ'ib qiladigan materiallarni tayyorlash vatarqatishidir. So'ngi yillarda terrorchilik tashkilotlarining g'oyalarini targ'ib qiladigan vauning materiallarini tarqatadigan veb-saytlarining soni 7000 dan oshgan. Asosan bunday veb-saytlarga tashrif beruvchilarning aksariyat qismi yoshlardir. Bunday materiallarni tarqatadiganlar hozirda ko'plab yoshlarni tashkil etmoqda.

Virtual olam orqali yengil pul topishni va to'kin-sochin hayot kechirishni o'zoldiga maqsad qilib olgan shaxslar virtual olamda firibgarlik qilish orqali o'zmablag'larini ko'paytirib bormoqda. Bunday firibgarlik qilishda asosiy rolni pulo'ynaydi, firibgarlar esa bu pullarni odamlardan olish usullarini esa juda yaxshibiladi. Bunda esa firibgarlar quyidagi jumlar yordamga keladi: "Siz uyda o'tirgan holdakiyimlar, maishiy-texnika vositalarini, taqinchoqlarini arzon narxlarda xarid qilishni xohlaysizmi?!" unda quyidagi link orqali telegram kanalimizga tashrif buyring vaxaridlar qiling bizda yetkazib berish xizmati ham mavjud. Mana shunday chiroyligaplardan foydalangan holda insonlarning pullarini o'zlashtirish bugungi kunda onlayn savdodagi firibgarlik nomi bilan mashhur. Shu o'rinda onlayn savdodagi firibgarliklarning qanday turlari mavjud va firibgarlar bu pullarni qandayo'zlashtirmoqda degan savol tug'iladi.

Ba'zi firibgarlar qalbaki, sifatsiz tovarlar, yoki mahsulotlar savdosi bilan shug'ullangan holda xaridorlarni chuv tushirsa, boshqalari mahsulot uchun oldindan qisman yoki to'liq to'lov qilishni talab qiladi. To'lov amalga oshirilgach xaridorga mahsulot yetkazilmaydi. So'ngi yillarda mamlakatimizda onlayn savdodagi firibgarlartomonidan jabrlanganlar soni tobora ortib bormoqda. Achinarlisi esa onlayn savdodagi firibgarlarni qo'lga olish va ularga jinoiy javobgarlik ochish deyarli imkonsiz sababi firibgarlar o'zining xavfsizligini va qo'lga tushib qolmasligini shunday ta'minlaganki hatto ularning kimligini aniqlash ham mushkul ish hisoblanadi. Firibgarlar o'zgalarnomiga yoki boshqa qandaydir telegram botlaridan foydalangan holda o'zlarigaijtimoiy tarmoqda profil yaratadi va shu profil orqali xaridorlar bilan muloqot qiladi. Xaridorlarga maxsulot yetib borishi uchun oldindan pulning yarmini yoki to'liqqismini to'lashni aytadi agar xaridor iloji boricha pulni ertaroq to'lasa tovarlar yetib kelishi ham tez bo'lishini aytadilar va ular gaplari oxirida yetkazib berish xizmatibepuligini va eshikkacha yetkazib berish xizmati mavjudligini aytadi. Bundan xursand bo'lgan, tovarlarini iloji boricha tezroq olishni xohlagan mijoz esa to'lovni tezda amalga oshiradi qarabsizki u firibgarlar qurboniga aylandi. Chunki hisobiga pultushganini ko'rgan firibgar tezda ijtimoiy



tarmoqdagi profilini o'chirib tashlaydi vako'zdan g'oyib bo'ladi. Xaridor esa jabrlanuvchi bo'lib qolaveradi.

Hozirgi kundagi virtual olamdagi eng global muammo bo'lgan jinoyatlardan biribu zararli viruslarni tarqatishdir. Hamma mobil aloqa vositalaridan foydalanuvchilargavirus tushunchasi juda yaxshi tanish. Bu kichik dastur bilan bir necha boruchrashishgan.

Virus-dasturchi tomonidan tuzilgan kompyuter ish faoliyatiga to'siq bo'ladigan hodisalarni keltirib chiqaradigan zararli dastur hisoblanadi. Bu dastur asosan internettarmog'I orqali foydalanuvchi kompyuteriga tushadi. Virus o'zini kompyuterlarda har xil tutadi. Ba'zi bir viruslar kompyuterlarnikerakmas fayllar bilan to'ldirsa yana boshqalari operativ xotirani ko'p qismini ishlatibkompyuterlarni qotirib qo'yadi viruslarning boshqa qismi esa kerakli fayllarni yokitizim fayllarini o'chirib kompyuterlarga zarar yetkazadi. Zararli viruslardanhimoyalalanish uchun barcha foydalanadigan qurilmalaringizni doimo ishonchliantivirus dasturi bilan muntazam yangilab turing. Antivirus dasturi butunqurilmangizni zararli dasturlar mavjudligini tekshirib turish imkonini beradi. Zararlidasturlarni erta aniqlash va uning tarqalishining oldini olish uchun qurilmalaringiznidoidimiy ravishda skanerlashga odatlaning. Agarda siz internetdan biror fayl yokidasturni yuklab olsangiz ochishdan oldin uni antivirus bilan tekshiring. Bunda sizgaWindows tizimi Microsoft Defender deb nomlangan o'z ichki bepul va ishonchliantivirus dasturiga ega dastur yordam beradi. Microsoft Defender dasturining sozlamalarini to'g'ri sozlash orqali qurilmangizni yanada mukammalroq himoya qilishingiz mumkin.

Virtual jinoyatni virtual dunyoda sodir etilgan jinoiy harakat sifatida ta'riflash mumkin -- odatda ommaviy ko'p o'yinchi onlayn rol o'ynash o'yinlari, MMORPG. Virtual jinoyatning ta'rifini tushunish uchun virtual jinoyatning oqibatlarini tasvirlash uchun "virtual" atamasining zamonaviy talqinini baholash kerak. Shu ma'noda, virtual jinoyatlar "haqiqiy jinoyat oqibatlarini keltirib chiqaradigan" onlayn harakatlarni tavsiflaydi, lekin keng tarqalgan bo'lib jinoiy javobgarlikka tortiladigan harakatlar deb hisoblanmaydi.

"Virtual jinoyat" atamasining bir qancha talqinlari mavjud. Bir olim virtual jinoyatni haqiqiy jinoyatning barcha sifatlariga ega bo'lishi zarurligi, deb ta'riflagan va shuning uchun u umuman jinoyatning yangi qismi emas ediVirtual jinoyatning real hayotiy oqibatlarini borligini isbotlash qiyin, shuning uchun u jinoiy javobgarlikka tortiladigan deb tan olinmaydi. Virtual jinoyatlarga misollar: o'g'irlik, jinsiy tajovuz, o'g'irlik, ter do'konlari qurish - bularning barchasi odatda virtual olamlar, metaverses va iqtisodlarda sodir bo'ladi.

Virtual olamda ko'plab muammolar bor, ammo eng asosiy jinoyatlar bilan shug'ullanib kelishimiz kerak. Firibgarlik, kiber jinoyatchilik, va viruslar kabi xavfsizlik muammolari virtual olamning hozirgi kunda ko'p uchraydigan muammolaridir. Firibgarlar plastik kartalar orqali odamlarning hisoblaridan moliyaviy zararlarni olib borishni talab qilishadi. "Fishing" deb nomlangan virtual firibgarlik usuli o'z tajribasiga ega firibgarlar bank kartalaridan maxfiy ma'lumotlarni olib, ularga zarar yetkazmoqda. Bunday firibgarlikni oldini olish uchun shaxsiy bank kartalari parollari va kodlarini hech kimga bermaslik zarur.

Boshqacha, onlayn savdodagi firibgarlar xaridorlarni qalbaki, sifatsiz tovarlar bilan chuv tushirib, ularni xavfsizlikka soladi. Ular onlayn savdo profilidan foydalanib, maxsulotlar yetkazilishi uchun to'lovlarni oldindan olishni talab qilishadi, lekin maxsulotlarni yetkazib bermaydi. Bu xil firibgarliklar qo'lga olinishi va ularga jinoiy javobgarlik ochilishi juda muhim. Bundan tashqari, zararli viruslar va kiber jinoyatchilik virtual olamning xavfsizligini ta'minlash uchun katta muammolar. Zararli dasturlar internet orqali kompyuterlarga o'rnatilib, foydalanuvchilarning maxfiy ma'lumotlarini olish, kompyuter tizimlariga zarar yetkazish va hokazo mumkin. Antivirus dasturlar va yaxshi sozlamalar bu holatlarni oldini olishda juda muhimdir. Bu muammolar bilan kurashish uchun, odamlarning xavfsizlikni



ta'minlashga va ma'lumotlarni himoya qilishga alohida e'tibor qaratish kerak. Maxfiy ma'lumotlarni himoya qilish uchun kerakli muhitozni o'rnatish, yaxshi antivirus dasturlar bilan kompyuterlarni himoya qilish va onlayn savdo jarayonlarida ehtiyotkor bo'lish juda muhimdir.

So'nggi bir necha yil davomida virtual olamdagi firibgarliklar soni bir nechabaravarga oshib ketganini kuzatishimiz mumkin. Mazkur jarayon bilan birqatorda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta'minlash muammosi ham mavjud, albatta. Bu eng dolzarb masalardan biri-kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo'lgan virtual olamdagi jinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Tahlillarga ko'ra, dunyo bo'ylab har yili 500 milliondan ortik kiber hujumlar uyushtiriladi. Har soniyada taxminan 12 nafar insondan biri virtual olamda sodir etilgan hujumlar qurboniga aylanmoqda. Amerika Qo'shma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Lyuksemburg kabi rivojlangan davlatlarda virtual olamdagi jinoyatlar ko'rsatkichi umumiy jinoyatchilikning 60-65 foizini tashkil etadi. O'zbekistonda ham so'nggi uch yilda bu turdagi jinoyatlar 8,3 baravarga ko'payib, hozirda umumiy jinoyatchilikning qariyb 5 foizini tashkilotmoqda. Jahonning 38 foiz yoshlari esa shafqatsizlik, zo'rovonlikni targ'ib etuvchi materiallar ta'siriga tushayotgan bo'lsa, yana bir qanchasi o'z joniga qasd qilishni targ'ib qiluvchi 9 mingdan ziyod saytlar orqali osongina jon taslim qilish "dars"larini o'rganishyapti. 2014-yilda chop etilgan hisobotda (McAfee homiyligida) jahoniqtisodiyotga yetkazilgan yillik zarar 445 milliard dollarni tashkil qilgan. Cybersecurity Ventures tomonidan 2016-yilgi hisobotda kiberjinoyatlar natijasida yetkazilgan global zararlar 2021-yilga kelib yiliga 6 trillion dollargacha oshishi, 2025-yilga kelib esa 10,5 trillion dollargacha ko'tarilishi taxmin qilinmoqda. 2018-yilda Strategik va Xalqarotadqiqotlar markazi (CSIS) tomonidan McAfee bilan hamkorlikda o'tkazilgan tadqiqotshuni ko'rsatadiki, har yili global YaIMning qariyb bir foizi ya'ni 600 milliard dollargayaqini virtual olamdagi jinoyatlar tufayli yo'qolar ekan.

Yuqoridagi statistik ma'lumotlar ko'rsatishicha, agar biz virtual olamdagi jinoyatchilikka qarshi kurashmasak va uning sodir etilishining oldini olmasak, bu raqamlar ortsa ortadiki lekin kamaymaydi. Shuning uchun, biz virtual olamda ijtimoiy tarmoqlardan foydalangan holda ehtiyot bo'lishimiz va iloji boricha o'z xavfsizligimizni ta'minlashimiz kerak. Virtual olam real dunyodan ancha uzoq bo'lgan o'zga bir olamdir, unga bog'lanib qolmasligimiz, virtual olamni real dunyodan farqli ravishda hayot kechirishimiz kerak. Virtual olamdagi firibgarliklar tuzog'iga tushmaslik uchun esa ijtimoiy tarmoqdagi xabarlarga va tanish kishilarga ishonib qolmaslik kerak. Agar o'z kelajagingizga befarq bo'lmasangiz, virtual olamdagi jinoyatchiliklarning oldini olishga birga harakat qilaylik va atrofimizdagi insonlarning virtual olmadagi firibgarlar qo'lga tushib qolmaslikka ogohlantiraylik.

Virtual olamdagi jinoyatlar, kiberxavfsizlikning muammosi, va kiberjinoyatlar statistik ma'lumotlari haqida maqola ko'rsatkichi, virtual olamda xavfsizlikni ta'minlashning muhimligi, va virtual olamdan o'z xavfsizligimizni himoya qilishning zarurati qayd etilgan. Yuqoridagi statistik ma'lumotlar, virtual olamdagi jinoyatchilikka qarshi kurashishning muhimligini ta'kidlaydi. Virtual olamda xavfsizlikni ta'minlash uchun ijtimoiy tarmoqdagi xabarlarga va notanish kimsalarga ishonib qolish, virtual olamdan real hayotga ajratib qolish, va jinoyatlar tuzog'iga tushmagan holda faol bo'lish, kiberxavfsizlikni ta'minlash uchun keng imkoniyatlarni yaratadi.

Virtual olamda ko'plab muammolar bor, ammo eng asosiy jinoyatlar bilan shug'ullanib kelishimiz kerak. Firibgarlik, kiber jinoyatchilik, va viruslar kabi xavfsizlik muammolari virtual olamning hozirgi kunda ko'p uchraydigan muammolaridir. Firibgarlar plastik kartalar orqali odamlarning hisoblaridan moliyaviy zararlarni olib borishni talab qilishadi. "Fishing" deb nomlangan virtual firibgarlik usuli o'z tajribasiga ega firibgarlar bank kartalaridan maxfiy ma'lumotlarni olib, ularga zarar yetkazmoqda. Bunday firibgarlikni oldini olish uchun shaxsiy bank kartalari parollari va kodlarini hech kimga bermaslik zarur.



Boshqacha, onlayn savdodagi firibgarlar xaridorlarni qalbaki, sifatsiz tovarlar bilan chuv tushirib, ularni xavfsizlikka soladi. Ular onlayn savdo profilidan foydalanib, maxsulotlar yetkazilishi uchun to'lovlarni oldindan olishni talab qilishadi, lekin maxsulotlarni yetkazib bermaydi. Bu xil firibgarliklar qo'lga olinishi va ularga jinoiy javobgarlik ochilishi juda muhim. Bundan tashqari, zararli viruslar va kiber jinoyatchilik virtual olamning xavfsizligini ta'minlash uchun katta muammolar. Zararli dasturlar internet orqali kompyuterlarga o'rnatilib, foydalanuvchilarning maxfiy ma'lumotlarini olish, kompyuter tizimlariga zarar yetkazish va hokazo mumkin. Antivirus dasturlar va yaxshi sozlamalar bu holatlarni oldini olishda juda muhimdir. Bu muammolar bilan kurashish uchun, odamlarning xavfsizlikni ta'minlashga va ma'lumotlarni himoya qilishga alohida e'tibor qaratish kerak. Maxfiy ma'lumotlarni himoya qilish uchun kerakli muhitni o'rnatish, yaxshi antivirus dasturlar bilan kompyuterlarni himoya qilish va onlayn savdo jarayonlarida ehtiyotkor bo'lish juda muhimdir.

FOYDALANILGAN INTERNET MATERIALLARI

1. https://www.google.com/search?q=virtual+olamdagi+jinoyatlar&oeq=virtual+olamdagi+jinoyatlar&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIGCAEQRRg80gEJMTQ5MTdqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8
2. https://en.wikipedia.org/wiki/Virtual_crime
3. https://en.wikipedia.org/wiki/Virtual_crime
4. kknews.uz
5. Zarnewz.u
6. Ибрахимов, Б. (2023). НИ ВЕСЕЛОВСКИЙ КАК ИССЛЕДОВАТЕЛЬ СРЕДНЕЙ АЗИИ. Interpretation and researches, 1(4).
7. G'ulomjonov, O. (2023). OILAVIY HUQUQLARNI AMALGA OSHIRISH VA OILAVIY MAJBURIYATLARNI BAJARISH. Namangan davlat universiteti Ilmiy axborotnomasi, (7), 856-860.
8. Абдуллаев, А. Н. (2020). SOCIAL AND ECONOMIC FACTORS OF COUVOLUTION PROBLEMS. Scientific Bulletin of Namangan State University, 2(8), 150-155.
9. Tolibjonovich, M. T., & Rahimjon o'g'li, G. O. (2021). Prerequisites For The Development Of A Leasing Mechanism In Public-Private Partnership. International Engineering Journal For Research & Development, 6 (SP), 5.
10. liv.uz
11. 4.cyberleninka.ru
12. uzreport.news
13. google.com
14. xs.uz
15. aniq.uz
16. istemol.uz
17. ishtixon.uz
18. yuridik.uz