MAVZU: INTERNET ORQALI SODIR ETILAYOTGAN JINOYATLARNING UMUMIY TAVSIFI, SODIR ETISH USULLARI VA ULARNI OLDINI OLISH CHORA-TADBIRLARI

Doniyorova Dinaraxon To`lqinovna
Ichki ishlar Vazirligi Akademiyasi kursanti

Annotatsiya:
Ushbu maqola orqali siz so'ngi yillarda O'zbekiston Respublikasida internet va AT (Axborot texnologiyalar) orqali sodir etilayotgan jinoyatlar va huquqbuzarliklarning umumiy tavsifi, sodir etish usullari, turlari, ko'rsatkichlari, jabrlanuvchilarning yo'l qo'ygan xatoliklari va oldini olish borasidagi amalga oshirilayotgan chora-tadbirlarni ko'rishingiz mumkin.

Kalit so'zlar: AOKA, AT, kiberjinoyat, kiberxavfsizlik, plastik kartalar, fishing, SMiShing, kibertovlamachilik, kiberbulling, davlat xizmatchisi, chip, fake xabarlar, mobil to'lov tizimi, maxsus kod, proksi sozlamalar, akkaunt, profil, treyderlik, ijtimoiy tarmoqlar, mobil o'yinlar, arzon buyumlar, kvalifikatsiya, NFS, IIO, HMQO, Profilaktika.

Annotation:
Through this article, you can see the general description of crimes and offenses committed in the Republic of Uzbekistan through the internet and AT (Information Technology) in recent years, methods of committing, types, indicators, measures taken to prevent the mistakes made by victims.

Keywords: AOKA, IT, cybercrime, cybersecurity, plastic cards, phishing, SMiShing, cyberbullying, cyberbullying, account, profil, civil servant,fake massages, chip, spemobile payment system, special massages, trading, social networks, mobile games, cheap items. qualification, NFS, IAB, LEA, Prevention.

Аннотация:
В данной статье вы можете ознакомиться с общим описанием преступлений и правонарушений, совершенных в Республике Узбекистан в последние годы через интернет и ИТ (информационные технологии), методами, видами, показателями совершения, ошибками потерпевших и мерами по их предупреждению.

Ключевые слова: АОКА, ИТ, киберпреступность, кибербезопасность, пластиковые карты, фишинг, СМиШинг, киберзапугивание, государственный служащий, аккаунт, профиль, настройки прокси, ложные сообщения, мобильная платежная система,

специальный код, трейдинг, социальные сети, чип, мобильные игры, дешевые товары. квалификация, NFS, ОВД, правоохранительные органы.

O'zbekiston Respublikasi AOKA (axborot va ommaviy kommunikatsiyalar agentligi) xabariga ko'ra hozirgi vaqtda yurtimizda 25 milliondan ortiq internet foydalanuvchisi mavjud. Ushbu raqamlar orasida internetdan g'arazli maqsadlardan foydalanayotgan shaxslar ham mavjud. So'ngi yillarda axborot-telekommunikatsiya vositalari orqali sodir etilayotgan jinoyatlar va huquqbuzarliklar soni salmoqli oshdi. Bu yil birgina Toshkent shahrining o'zida **4332 ta** AT orqali sodir etilgan jinoyatlar aniqlangan. Bu ko'rsatkich 2021-yilga **(2281 ta)** qaraganda **2** baravarga, 2020-yil **(106 ta)** bilan taqqoslaganda esa, **40** baravarga ko'pdir.

Jinoyatlarni tahlil qilishdan oldin Kiberjinoyatchilik, Kiberhujum, Kiberhimoya va Kiberxavfsizlik tushunchalariga qisqa ta'rif beradigan bo`lsak:

Kiberjinoyatchilik[1]— axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig'indisidir.

Kiberhujum[1] — kibermakonda apparat, apparat-dasturiy va dasturiy vositalardan foydalangan holda qasddan amalga oshiriladigan, kiberxavfsizlikka tahdid soladigan harakat.

Kiberhimoya[1] — kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarni aniqlashga va ulardan himoya qilishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommunikatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar, shuningdek ma'lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlari majmui.

K**iberxavfsizlik**— kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati.

Yuqoridagi jinoyatlarning ko'pgina qismi og'irlik va firibgarlik orqali sodir etilgan. Bugungi kunda ularni **Fishing, SMiShing, Kiberbulling, Kibertovlamachilik** kabi turlari mavjud. Xo'sh, aslida ular nimani anglatadi?

Fishing — (**Phishing**) — Firibgarlikning bir turi bo`lib, bu asosan elektron pochtalarga feyk (fake) xabarlar yuborish orqali amalga oshiriladi. Ya'ni ushbu xabar ortida zararli dastur yoki virus joylashgan bo'ladi. Shundan so'ng huquqbuzar foydalanuvchining shaxsiy ma`lumotlaridan noqonuniy foydalishni boshlaydi.

[1] 2022-yil 15-apreldagi "Kiberxavfsizlik to`g`risida" gi 764-son O`RQ ning 3-modda 3-6-10-11-bandlari.

SMiShing — Fishingning bir turi bo'lib, undan farqli jihati, faqatgina qurilmalarning SMS xabarnomasiga kelishidadir va shu boisdan ham ko'pchilik fuqarolar yuqoridagi ikki jinoyatni adashtirish holatlari kuzatilmoqda.

Kibertbulling — raqamli texnologiyalar yordamida, foydalanuvchilarning shaxsiy yoki yolg'on ma`lumotlar bilan sharmanda qilish, qo`rqitish yoki tahdid qilishdir.

Kibertovlamachilik — Internet yoki telekommunikatsiya vositalari orqali fuqarolarning shaxsiy ma'lumotlarini tarqatish bilan tahdid qilib moddiy mablag' talab qilish bilan bog'liq jinoyat.

2022-yil internet tarmoqlari va AT orqali sodir etilgan jinoyatlar orqali jabrlanuvchilar jami bo`lib **45 mlrd 215 mln** so'm moddiy zarar ko'rdi. Ulardan **9 mlrd 16 mln**[1] so'm undirilib berildi.

2022-yilda Toshkent shahrida AT orqali sodir etilayotgan jinoyatlarning ko'rsatgichi[2]:

O'g'irlik: 63%;

Giyohvandlik savdosi: 20%;

Firibgarlik: 15%;

Boshqa turdagi kiberjinoyatlar: 2%.

Huquqbuzarliklarni sodir etish usullari. Yuqoridagi jinoyatlar asosan fuqarolarning soddaligi va ishonuvchanligi, shu bilan birgalikda texnikaviy savodxonligi pastligidan foydalanib sodir etilmoqda. Ko'rsatkichlarga e'tibor beradigan bo'lsak, jami kiberjinoyatlarning **60%** dan ortig'ini **SMiShing** tashkil etmoqda. Xo'sh, aynan ushbu jinoyatning yurtimizda avj olib ketishiga nimalar sabab bo'lmoqda. Ushbu savolga subyektiv jihatdan yondashadigan bo`lsak:

Fuqarolar nuqtai nazaridan: jinoyatchi o'zini "bank hodimi" yoki "davlat xizmatchisi" deb tanishtiradi va jabrlanuvchining plastik kartasiga kiberhujum bo'layotganini, agar SMS orqali borgan kodni aytmasa pullari o'g'irlanishi yoki bloklanib qolishi mumkinligini aytib o'tadi. Fuqaro esa o'z navbatida telefonga kelgan maxsus kodni "bank hodimi"ga aytadi;

HMQO (Huquqni muhofaza qiluvchi organlar) hodimlari tomonidan ushbu turdagi jinoyatlarga nazar soladigan bo'lsak, ko'p hollarda plastik kartalardan yechib olinayotgan pul mablag'lari asosan bir nechta kartalarga, hatto chet el hisob raqamlariga ham o'tkazilib, o'g'irlash holatlari kuzatilmoqda. Bu esa jinoyatlarni ochishda va ularni kvalifikatsiya qilishda ko'pgina jiddiy muammolarni va qarama-qarshiliklarni keltirib chiqarmoqda. Ya'ni karta raqami egasi ma'lumotlari maxfiy hisoblanib, ularni olish uchun sanksiya talab etiladi. Bu esa o'z navbatida vaqtni talab qiladi. Ushbu vaqt ichida esa pullar yana o'nlab kartalarga o'tadi.

[2] https://www.gazeta.uz/oz/2023/02/21/cyber

Shuni ham inobatga olish kerakki, o'tkazilgan har bir kartaning egasi **huquqbuzar** bo'lishi mumkin. O'ylaganingizdek, ularning har birini aniqlab chiqish yetarlicha vaqtni talab qiladi.

Keyingi masala, chet el hisob raqamlariga chiqqan pul mablag'lari yuzasidan. Chet el fuqarolarining bank hisobi ma'lumotlarinin olish imkoni yo'qligi bois, qabul qilingan va o'tkazilgan pul mablag'larini aniqlash mushkul. Shu boisdan jinoyatlarni ochishda bir qancha muammolar yuzaga kelmoqda.

Shu bilan birgalikda fuqarolarning quyidagi xatolari tufayli ham boshqa turdagi kiberjinoyatlar sodir etilmoqda:

Ya'ni, ijtimoiy tarmoqlar orqali foizsiz to'lovlar, kreditlar, davlat tomonidan ijtimoiy pul yordami berilayotgani, arzon narxdagi buyumlar savdosi yoki soxta saytlarga ro'yxatdan o'tish va shuning orqasidan fuqarolarning pulini o'zlashitirish holatlari;

Mobil va boshqa turdagi o'yinlarga pul tikuvchi yoki o'tkazib beruvchi soxta saytlar, treyderlik bilan shug'ullanuvchi shaxslarga soddalik bilan pul o'tkazish va boshqalar.

Kiberjinoyatlardan saqlanish usullari:

− Plastik kartangizni raqamini va muddatini boshqa kimsalarga aytmang. Hattoki bank hodimlariga ham, chunki bank ma'lumotlar bazasida sizning barcha ma'lumotlaringiz, shu jumladan raqamlaringiz ham mavjud.

− Deyarli barcha banklarning xavfsizlik tizimi shunday tuzilganki, u yerdan sizning ma'lumotlaringizni olish faqatgina sizning telefoningizga kelgan maxsus kod orqali amalga oshiriladi. Shu maqsadda maxsus kodni hech kimga aytmang.

− Shu bilan birga plastik kartalaringizni qattiq g'iloflarda saqlang. Hozirda mini NFS qurilmalari orqali masofadan pul o'g'irlash holatlari ham aniqlanmoqda.

− Elektron pochta va akkauntlaringizga qiyinroq bo'lgan kod qo'ying va 2 bosqichli himoya tizimidan foydalaning.

− Internet orqali o'tkaziladigan pul mablag'larini faqatgina rasmiy va ishonchli saytlar yoki ilovalar orqali amalga oshiring.

− Turli xil mahsulotlar xarid qilishni faqat rasmiy saytlar orqali amalga oshiring

− Internet yoki AT vositalari orqali sizga kibertovlamachilik yoki qo'rqitish, tahdid[1] **(kiberbulling)** qilish holatlari bo'lsa zudlik bilan IIO (Ichki Ishlar Organlari) ga xabar bering.[3]

Internet va AT orqali sodir etilayotgan jinoyatlarni oldini olish borasida IIO hodimlarining ustuvor vazifalari.

− Fuqarolarning kiber va texnikaviy ongini rivojlantirish maqsadida uzviy tarzda targ'ibot ishlarini olib borish;

− Aynan qaysi ko'rinishdagi kiberhuquqbuzarliklar ko'proq sodir etilayotganligi yuzasidan fuqarolarni doimiy ravishda ogohlantirib borish;

[3] **kibertahdid**— kibermakonda shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui: 2022-yil 15-apreldagi "Kiberxavfsizlik to'g'risida" gi 764-son O`RQ ning 3-moddasi 5-bandi.

– Internet va AT vositalari orqali sodir etiladigan huquqbuzarliklardan saqlanish borasidagi chora-tadbirlar haqida ma’lumotlatlar berish.

Zamonaviy raqamli dunyoda plastik kartaning to‘lov tafsilotlari, bank foydalanuvchilarining login va parollari, foydalanuvchilarning ma’lumotlari, bank hisob varaqlari, moliyaviy ma’lumotlar va shu turdagi ma’lumotlar firibgarlarda juda katta qiziqish uyg‘otadi. Ma’lumotlaringizni aniqlash uchun, firibgarlar turli xil usullardan foydalanishadi. Misol tariqasida, elektron pochta xabarlarini (spam) hamda phishing veb-saytlarni ommaviy ravishda tarqatish.

Phishing – (inglizcha Fishing so‘zidan olingan bo‘lib, baliq ovlash degan ma’noni anglatadi), bu maxfiy ma’lumotlarni o‘g‘irlash uchun ishlatiladigan keng tarqalgan usullardan biridir.

Bugungi kunda O‘zbekiston Respublikasi hududida ham phishing veb-saytlar orqali foydalanuvchilarni chuv tushurish holatlari keng kuzatilmoqda. Firibgarlar foydalanuvchilarning ishonchini qozonish maqsadida turli xil rasmiy veb-saytlarni nusxasini yaratishdan, jumladan, O‘zbekiston Respublikasi Prezidentining rasmiy veb-sayti www.prezident.uz, banklar va shu turdagi tashkilotlarning rasmiy veb-saytlarini qalbaki ko‘rinishini yaratishdan keng foydalanishmoqda.

Bu turdagi phishing veb-saytlarga aldanib qolmaslik uchun avvalambor fuqarolardan ogoh bo‘lishlari talab etiladi. Shuningdek, phishing veb-sahifalarni tanib olish va haqiqiy veb-saytdan ajratish uchun quyidagi tavsiyalarga amal qilishlari maqsadga muvofiq:

Veb-saytning URL (domen) manziliga e’tibor bering. Phishing veb-saytning URL manzili rasmiy veb-resurs bilan juda o‘xshash bo‘ladi, ammo albatta farq qiladi; Ishonchsiz bo‘lgan manbalarga shaxsiy ma’lumotlaringizni (bank hisob raqamlaringizni, plastik karta raqamlaringizni, shaxsingizni tasdiqlovchi hujjatlaringiz ma’lumotlarini hamda parol va loginlaringizni) taqdim etmang;

Shaxsiy telefon raqamingizga kelgan tasdiqlash kodlarini begona shaxslarga bermang;

Shu turdagi phishing veb-saytlarga duch kelsangiz “Kiberxavfsizlik markazi” davlat unitar korxonasiga xabar bering.

“Kiberxavfsizlik markazi” davlat unitar korxonasi tomonidan joriy 2022-yil mobaynida moliyaviy firibgarlik bilan bog‘liq bo‘lgan 39 ta phishing veb-sahifalar aniqlandi hamda O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi bilan hamkorlikda bu veb-sahifalar faoliyati O‘zbekiston Respublikasi hududida cheklandi. Quyida so‘ngi aniqlangan Phishing veb-sahifalardan ba’zi namunalar keltirib o‘tiladi

Xulosa o’rnida shuni aytish lozimki, so’ngi yillarda yurtimizda olib borilayotgan islohotlar zamirida fuqarolarning kiber va texnikaviy madaniyatini oshirishga qaratilgan chora-tadbirlar yotibdi. Shu o’rinda eslatib o’tish kerakki, yuqorida ko’rsatilgan profilaktik qoidalarga amal qilish, kelgusida kiberjinoyatlar qurboniga aylanmaslik garovidir.

Foydalanilgan adabiyotlar

1. 2022-yil 15-apreldagi “Kiberxavfsizlik to’g’risida” gi 764-son O’RQ.
2. Vazirlar Mahkamasining 2018 yildagi «Butunjahon internet tarmog’ida axborot xavfsizligini yanada takomillashtirish chora-tadbirlari to’g’risida"gi 707-sonli qarori.
3. 2001-yil 8-noyabrdagi 109-sessiyada qabul qilingan “Kiberjinoyatlar to’g’risida” konvensiya.
4. https://aoka.uz
5. https://iiv.uz
6. https://csec.uz/uz/
7. https://www.gazeta.uz

Ilmiy rahbar – leytenant Axmedov Xamidulla Xayrullo o‘g‘li, IIV Akademiyasi Axborot texnologiyalari kafedrasi O’.M.K boshlig’i