



## AXBOROT SOHASIDAGI KIBERJINOYATCHILIKNING OMMAVIY TARQALGAN SHAKLLARIDAN HIMOYALANISH USULLARI

**Raxmonov Shaxobiddin Shuxrat o'gli**

Buxoro viloyati IIB huzuridagi Tergov Departamenti

G'ijduvon tuman IIB huzuridagi Tergov bo'linmasi tergovchisi

<https://www.doi.org/10.5281/zenodo.10574481>

### ARTICLE INFO

Received: 18<sup>th</sup> January 2024

Accepted: 25<sup>th</sup> January 2024

Online: 27<sup>th</sup> January 2024

### KEY WORDS

### ABSTRACT

*Maqolada muallif tomonidan kiberjinoyatning eng keng tarqalgan shakllaridan himoya qilishga yordam beradigan ba'zi ehtiyot choralari keltirilgan.*

Butun dunyoda hozirgi kunda jinoyatchilikning yangi turlari jinoyat sodir etishning yangi usullari va shakllari yaratilmoqda. Bunga kiberjinoyatchilikning ommaviy tarqalishini yorqin misol sifatida keltirishimiz mumkin.

O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashish haqida bir qator ishlar amalga oshirilmoqda. Hususan, O'zbekiston Respublikasining 2022 yil 15 aprelidagi "Kiberxavfsizlik to'g'risida"gi 764-sonli<sup>1</sup> Qonuni bunga yorqin misol bo'la oladi. Bundan tashqari, O'zbekiston Respublikasi Davlat xavfsizlik xizmati raisining 2023 yil 4 sentyabrdagi "O'zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi ob'ektlarining kiberxavfsizligini ta'minlash darajasini baholash tartibi to'g'risidagi nizomni tasdiqlash haqida"gi 91-sonli buyrug'i asosida, O'zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi ob'ektlarining kiberxavfsizligini ta'minlash darajasini baholash tartibi to'g'risidagi nizom tasdiqlangan<sup>2</sup>.

Ushbu qiberxavfsizlikni ta'minlash bo'yicha qabul qilingan huquqiy asoslar bilan hozirgi kunda kiberjinoyatlarning oldi olinmoqda. Ammo qilinayotgan ishlarning yetarli darajada yemasligi sababli, O'zbekiston Respublikasida 2023 yilning 11 oyida 5,5 mingta kiberjinoyat sodir etilgan.

O'tgan 11 oyda 5,5 mingta kiberjinoyat sodir etilgan bo'lsa, shundan 70 foizi bank kartalari bilan bog'liq firibgarlik va o'g'irlik jinoyatlari hisoblanadi.

Bugungi kunda mamlakatimizda 50 ga yaqin to'lov tizimi bo'lib, ularning hammasi ham kiberxavfsizlik talablariga javob bermasligi qayd etildi.

Noyabr oyida IT vositasida sodir etiladigan huquqbuzarliklarga qarshi kurashish bo'yicha Prezident qarori imzolandi.

<sup>1</sup> <https://lex.uz/docs/5960604> "Kiberxavfsizlik to'g'risida"gi O'RQ-764-son qonun (murojaat vaqti: 22.01.2024y.).

<sup>2</sup> [https://nrm.uz/products?folder=230131\\_ahborot\\_havfsizligi&products=1\\_vse\\_zakonodatelstvo\\_uzbekistana](https://nrm.uz/products?folder=230131_ahborot_havfsizligi&products=1_vse_zakonodatelstvo_uzbekistana) (murojaat vaqti: 22.01.2024y.).



Mutasaddi vazirlik va idoralarga barcha elektron to'lov tizimlari uchun yagona kiberxavfsizlik talablarini ishlab chiqish va ijrosini qat'iy nazorat qilish lozim<sup>3</sup>.

Shaxsni o'g'irlash boshqa shaxsning shaxsiy ma'lumotlaridan noqonuniy faoliyatni amalga oshirish uchun foydalanishni o'z ichiga olgan jinoyatdir. Ushbu turdagi kiberjinoyat sizning shaxsiy ma'lumotlaringiz o'g'irlanganda va jinoyatchilar tomonidan moliyaviy foyda olish uchun foydalanilganda sodir bo'ladi.

Bu erda shaxsni o'g'irlashning eng keng tarqalgan shakllari:

Moliyaviy identifikatsiyani o'g'irlash: kredit kartalari, bank hisob raqamlari, ijtimoiy sug'urta raqamlari va boshqalardan ruxsatsiz foydalanish.

Shaxsiy identifikatsiyani o'g'irlash: shaxsiy ma'lumotlaringizdan elektron pochta hisoblarini ochish va onlayn narsalarni sotib olish kabi noqonuniy faoliyatni amalga oshirish uchun foydalanish.

Soliq identifikatorini o'g'irlash: noto'g'ri soliq deklaratsiyasini topshirish uchun ijtimoiy sug'urta raqamingizdan foydalanish.

Tibbiy shaxsni o'g'irlash: tibbiy xizmatlarga murojaat qilish uchun shaxsiy ma'lumotlaringizdan foydalanish.

Ish joyini o'g'irlash: noqonuniy faoliyatni amalga oshirish uchun ish joyingiz profili ma'lumotlarini o'g'irlash.

Bolaning shaxsini o'g'irlash: bolangiz ma'lumotlaridan noqonuniy harakatlar uchun foydalanish.

Katta yoshdagi shaxsni o'g'irlash: moliyaviy jinoyatlar uchun keksa fuqarolarning shaxsiy ma'lumotlarini o'g'irlash.

Shaxsni o'g'irlashdan qanday qochish kerak.

Shubhali harakatlar bo'lmasligi uchun bank hisoblaringizni tez-tez tekshirib turing.

Ijtimoiy sug'urta kartangizni hamyoningizda olib yurmang.

Agar kerak bo'lmasa, shaxsiy ma'lumotlaringiz va fotosuratlaringizni Internetda noma'lum shaxslarga baham ko'rmang

Barcha hisoblar uchun bir xil paroldan foydalanishdan saqlaning.

Katta va kichik harflar, raqamlar, belgilar va boshqalarni o'z ichiga olgan kuchli parollar yarating.

Har bir hisob qaydnomangizda ikki faktorli autentifikatsiyani yoqing.

Parollaringizni tez-tez o'zgartiring.

Shaxsiy ma'lumotlarni o'g'irlashdan himoya qilishni o'z ichiga olgan antivirus dasturidan foydalaning.

Har qanday firibgarlik belgilarini aniqlash uchun kredit balingizni va tranzaktsiyalaringizni kuzatib boring.

Fishing jinoyatchilar tomonidan bank hisob raqamlari, parollar va hokazo shaxsiy ma'lumotlaringizga kirish uchun qo'llaniladigan eng keng tarqalgan ijtimoiy muhandislik sxemalaridan biridir. Siz qilishingiz kerak bo'lgan yagona narsa havolani bosish, lekin bu sizni muammoga duchor qilish uchun yetarli. . Sizning bank hisobingiz ma'lumotlarini onlayn tarzda tekshirish so'ralganda, xakerlar foydalanuvchilarga eng ishonchli ko'rinadigan havolalarni

<sup>3</sup> <https://www.gazeta.uz/uz/2023/12/21/cyber-crime/> (murojaat vaqti: 22.01.2024й.).



bosishni maslahat berishadi. Ko'pchilik noma'lum jo'natuvchilar tomonidan yuborilgan havolalarni bosish yoki fayllarni ochish bilan bog'liq tahdidlardan xabardor emasligi sababli, ular qurbon bo'lib, pullarini yo'qotadilar.

O'zingizni fishingdan qanday himoya qilish kerak.

Fishingdan qochish uchun siz bosayotgan havolalardan ehtiyot bo'lishingiz va har doim bu qonuniy xabar yoki yo'qligini ikki marta tekshirishingiz kerak. Shuningdek, brauzeringizni oching va noma'lum jo'natuvchi tomonidan yuborilgan havolalarni bosish o'rniga to'g'ridan-to'g'ri bank hisobingizga kiring.

Ransomware - bu fayl va hujjatlaringizni qulflaydigan yoki shifrlaydigan va ularni asl holiga qaytarish uchun pul talab qiladigan zararli dastur turi. Bepul dekodlash vositalari mavjud bo'lsa-da, ko'pchilik qurbonlar to'lovni to'lashni afzal ko'rishadi, chunki bu muammodan eng tez chiqish yo'lidir.

O'zingizni to'lov dasturidan qanday himoya qilish kerak.

To'lov dasturidan qochish uchun siz elektron pochta yoki veb-saytlar orqali nima ochayotganingiz va bosayotganingizga juda ehtiyot bo'lishingiz kerak. Hech qachon noma'lum jo'natuvchilardan elektron pochta xabarlarini yoki fayllarni yuklab olishingiz va shubhali havolalar va reklamalardan qochishingiz kerak, ayniqsa ular sizni odatda bepul xizmatlar uchun to'lashga majbur qilganda. Onlayn ta'qib, kibertalking va bezorilik Onlayn ta'qib va zo'ravonlik ko'p sonli kiberjinoyatlarni hisobga oladi va u asosan nom qo'ng'iroq qilish yoki kiberbullying bilan boshlanadi, lekin asta-sekin onlayn ta'qib va o'z joniga qasd qilish tahdidlariga aylanadi. AQSh Adliya Statistikasi Byurosining ma'lumotlariga ko'ra, har to'rt boladan 1 nafari kiberbullying qurboni bo'ladi. Depressiya, tashvish, o'zini past baho va boshqalar kabi psixologik ta'sirlar bu jinoyatlarning asosiy oqibatlaridir. Qanday qilib onlayn ta'qib va zo'ravonlikdan himoyalaniish kerak Agar kimdir sizni onlayn tarzda bezovta qilayotganini his qilsangiz, ularni bloklash suiste'mollikni to'xtatishga va ruhiy sog'lig'ingizga zarar yetkazmaslikka yordam beradi. Ijtimoiy media platformalarida va internet orqali shaxsiy ma'lumotlaringizni begonalar bilan baham ko'rishdan saqlaning. Xavfsizlik dasturini yangilab turing va hisoblaringizni himoya qilish uchun ikki faktorli autentifikatsiyadan foydalaning. O'zingizni noqulay yoki asabiylashtiradigan xabarlariga javob bermang, ayniqsa ular jinsiy aloqada bo'lsa. Faqat ularni o'chirib tashlang. Facebook, Instagram, Twitter va boshqalar kabi ijtimoiy media platformalari o'z veb-saytlarida har qanday turdagi ta'qiblarga toqat qilmaydi va siz ularning xabarlarini ko'rmaslik uchun ushbu saytlarda odamni bloklashingiz mumkin. Firibgarlik va firibgarlik Onlayn savdo - bu istiqbolli biznesdir. Biroq, siz ularga pul yuborishingizni va shaxsiy ma'lumotlarni oshkor qilishni xohlaydigan firibgarlar va firibgarlarga e'tibor berishingiz kerak. Ba'zi standart onlayn firibgarlik usullari: Phishing: login ma'lumotlarini yoki kredit karta raqamlarini so'rash uchun o'zini rasmiy veb-sayt sifatida ko'rsatuvchi xabarlarini yuborish. Soxta tasdiqlar: xabarlar qoniqarli mijozlardan kelganga o'xshaydi, lekin aslida sizning kompyuteringizga yoki shaxsiy ma'lumotlaringizga zarar yetkazadigan mahsulot va xizmatlarni sotib olishingizni xohlaydi.

Kriptoalyuta firibgarligi: kriptoalyutalarga sarmoya kiritishingizni va ularning hisoblariga pul o'tkazishingizni so'raydi, chunki ular katta foyda olishlari mumkin. Shaxsni o'g'irlash: ta'lim, viza masalalari va hokazolar uchun oldindan ma'lum miqdorda pul to'lashni talab qiladigan ishlarni taklif qilish.



Xorijda kiberjinoyatda ayblangan shaxsga qanday jazo tayinlanadi? Dubayda kiberjinoyatchilar, jumladan, qattiq jazoga tortilishi mumkin jarimalar, qamoq muddati va hatto ba'zi hollarda o'lim jazosi. Shaxsga qanday jazo tayinlanishi jinoyatning og'irligiga va ishning tafsilotlariga bog'liq bo'ladi.

Misol uchun, firibgarlik yoki boshqa moliyaviy jinoyatlarni sodir etish uchun kompyuterdan foydalanganlikda ayblangan shaxs katta miqdordagi jarima va qamoq jazosiga, terrorizm kabi og'irroq jinoyatlarda ayblanganlarga esa o'lim jazosi berilishi mumkin. Onlayn firibgarlik va firibgarlikdan qochish bo'yicha maslahatlar Hisoblarining himoya qilish uchun 2 faktorli autentifikatsiyadan foydalaning. Tranzaksiyadan oldin siz bilan yuzma-yuz uchrashishni istamaydigan odamlarni kuzatib boring. Shaxsiy ma'lumotlarni so'ragan shaxs yoki kompaniya haqida etarli ma'lumotga ega bo'lmasdan oshkor qilmang. Siz tanimagan odamlarga pul o'tkazmang. Agar xabarda login ma'lumotlaringiz yoki kredit karta raqamlaringiz so'ralsa, o'zlarini mijozlarga xizmat ko'rsatish vakili deb da'vo qilayotgan odamlarning xabarlariga ishonmang.

Kiberterrorizm kompyuter va internetdan foydalangan holda tartibsizlik, iqtisodiy zarar, qurbonlar va hokazolarni keltirib chiqarish orqali keng tarqalgan qo'rquvni yuzaga keltiruvchi qasddan qilingan harakatlar deb ta'riflanadi. Ushbu jinoyatlar veb-saytlar yoki xizmatlarga ommaviy DDoS hujumlarini boshlash, kriptovalyutalarni qazib olish uchun zaif qurilmalarni o'g'irlash, muhim infratuzilmaga (elektr tarmoqlariga) hujum qilish va hokazolarni o'z ichiga olishi mumkin. Kiberterrorizmdan qochish bo'yicha maslahatlar Xavfsizlik dasturi, operatsion tizim va boshqa qurilmalaringiz eng so'nggi versiyalarga yangilanganligiga ishonch hosil qiling. Atrofingizdagi shubhali xatti-harakatlarga e'tibor bering. Agar guvoh bo'lsangiz, darhol huquqni muhofaza qilish organlariga xabar bering. Umumiy Wi-Fi tarmoqlaridan foydalanishdan saqlanib, chunki ular fishing va odam-in-the-middle (MITM) hujumlari kabi hujumlarga ko'proq moyil. Maxfiy ma'lumotlarning zaxira nusxasini yarating va iloji boricha ularni oflayn rejimda saqlang. Kiberurush - bu internet yoki boshqa kompyuter tarmog'i orqali boshqa davlat yoki tashkilotga qarshi kiberfazoda olib boriladigan axborot urushining bir turi. Bunga razvedka ma'lumotlarini to'plash, jamoatchilikka ta'sir qilish uchun targ'ibot qilish uchun kiber josuslikdan foydalanish orqali erishish mumkin. Kiber jinoyatlar bo'yicha advokatlar bilan bog'laning Kiberjinoyatlarga qarshi kurashish qiyin, chunki ular Internet orqali sodir bo'ladi. Bu ham yangi va ko'p mamlakatlarda bunday hollarda nima qilish mumkinligi haqida aniq qonunlar mavjud emas, shuning uchun agar sizda shunga o'xshash narsa bo'lsa, chora ko'rishdan oldin advokat bilan gaplashgan ma'qul! Kiber jinoyatlar bo'yicha malakali advokatlar Amal Xamis advokatlari va yuridik maslahatchilar Dubayda sizning vaziyatingiz haqida sizga maslahat berishi va huquqiy jarayonda sizga rahbarlik qilishi mumkin. Kiberjinoyatlar bilan bog'liq savollaringiz bo'lsa, maslahat olish uchun bugun biz bilan bog'laning!

## References:

1. "Kiberxavfsizlik to'g'risida"gi O'RQ-764-son qonun <https://lex.uz/docs/5960604>



2. ўғли Насиров И. С. Рецидив жиноятчиликлнинг криминалогик тавсифи //ta'lim va rivojlanish tahlili onlayn ilmiy jurnali. – 2022. – С. 364-380.
3. [https://nrm.uz/products?folder=230131\\_ahborot\\_havfsizligi&products=1\\_vse\\_zakonodatelstvo\\_uzbekistana](https://nrm.uz/products?folder=230131_ahborot_havfsizligi&products=1_vse_zakonodatelstvo_uzbekistana) (мурожаат вақти: 22.01.2024й.).
4. Насиров И., Мухиддинов М. Шахснинг ҳаётига қарши қаратилган жиноятларнинг ҳозирги кундаги ҳолати //Академические исследования в современной науке. – 2023. – Т. 2. – №. 16. – С. 109-116.
5. <https://www.gazeta.uz/uz/2023/12/21/cyber-crime/> (мурожаат вақти: 22.01.2024й.).
6. Абдурасулова К. Мамлакатимизда криминалогик таълимотларнинг шаклланиши, ривожланиши, ҳозирги ҳолати ва замонавий криминалогия фанининг вазифалари //Общество и инновации. – 2021. – Т. 2. – №. 5. – С. 78-90.
7. <https://academy.binance.com/en/articles/what-is-the-metaverse>
8. ўғли Насиров И. С. Вояга етмаганлар ўртасида ҳуқуқбузарликларни олдини олиш масалалари //barqarorlik va yetakchi tadqiqotlar onlayn ilmiy jurnali. – 2022. – С. 212-215.