

KOMPYUTER TEXNIKA VOSITALARI ORQALI SODIR ETILGAN FIRIBGARLIK JINOYATI TURLARI

Suyunov Shaxzodbek Shovkatovich

O'zbekiston Respublikasi IIV Akademiyasi "Tergov faoliyati" kafedrası o'qituvchisi

Abduraimov Jasurbek Nusratullo o'g'li

O'zbekiston Respublikasi IIV Akademiyasi Tergov faoliyati mutahassisligi 3-bosqich
319-guruh kursanti

<https://doi.org/10.5281/zenodo.8019653>

Annotatsiya Mazkur maqola kompyuter texnika vositalari orqali sodir etilgan firibgarlik jinoyatlarini ko'rib chiqqan holda tahlil qilingan. Bundan tashqari, ushbu maqolada kompyuter texnika vositalari orqali sodir etilgan firibgarlik jinoyatlarga qanday turdagi jinoyatlar kirishini hamda uni oldini olish haqida so'z yuritamiz. [1]

Kalit so'zlar: kompyuter texnika vositalari, jinoyat, firibgarlik jinoyati,
KIRISH

"Kompyuter texnikasi yordamida sodir etilgan firibgarlik jinoyati" deganda jismoniy shaxsning boshqa shaxs yoki yuridik shaxsni moliyaviy manfaatlar yo'lida aldash maqsadida kompyuter texnikasidan foydalanishi bilan bog'liq jinoiy harakat tushuniladi. Bu shaxsiy ma'lumotlarni o'g'irlash, soxta veb-saytlar yoki akkauntlar yaratish, moliyaviy operatsiyalarni manipulyatsiya qilish yoki elektron vositalar orqali amalga oshirilgan aldashning boshqa shakllarini o'z ichiga olishi mumkin. Ushbu jinoyat uchun jazoning og'irligi amalga oshirilgan aniq harakatlarga va jabrlanuvchiga yetkazilgan zararga bog'liq bo'ladi. Shaxsiy ma'lumotlarni internetda baham ko'rishda ehtiyot bo'lish va har qanday shubhali firibgarlik holatlarini rasmiylarga xabar qilish muhim. "Kompyuter firibgarligi jinoyati" odatda kompyuter yoki internetdan foydalangan holda amalga oshirilgan har qanday jinoiy faoliyatni nazarda tutadi, masalan, xakerlik, identifikator o'g'irlash, fishing firibgarliklari va zararli dastur yoki viruslarni tarqatish. Bu jinoyatlar jismoniy shaxslar, korxonalar va hatto hukumatlarga jiddiy zarar yetkazishi va moliyaviy yo'qotish, ma'lumotlar o'g'irlanishi yoki kompyuter tizimlariga zarar yetkazishi mumkin. Kompyuter firibgarligi jinoyatlariga oid qonunlar yurisdiksiyaga qarab farq qiladi, lekin umuman olganda, ular noqonuniy hisoblanadi va katta jazolarni o'z ichiga oladi. Jinoyatning og'irligiga qarab, aybdorlar jarima, qamoq yoki har ikkalasiga ham tortilishi mumkin. Jismoniy shaxslar va korxonalar kuchli parollardan foydalanish, dasturiy ta'minotni yangilab turish va virusga qarshi dasturlardan foydalanish kabi kompyuter firibgarligi jinoyatlaridan o'zlarini himoya qilish choralarini ko'rishlari zarur.

ADABIYOTLAR TAHLILI VA METADALOGIYASI

"Kompyuter firibgarligi jinoyati" shuningdek, maxfiy ma'lumotlarni o'g'irlash yoki kompyuterning normal ishlashini buzish kabi noqonuniy maqsadlarda kompyuter yoki kompyuter tizimiga ruxsatsiz kirish huquqiga ega bo'lgan jinoyatni ham nazarda tutishi mumkin. Bunga tarmoqqa buzib kirish, parollarni o'g'irlash yoki tizimni boshqarish uchun zararli dasturlardan foydalanish kiradi. Potentsial moliyaviy yo'qotishlar yoki kompyuter tizimlariga etkazilgan zarardan tashqari, kompyuter firibgarligi jinoyatlari ham jiddiy huquqiy oqibatlariga olib kelishi mumkin. Jinoyatning tabiati va darajasiga qarab, aybdorlar turli qonunlar, jumladan, Qo'shma Shtatlardagi Kompyuter firibgarligi va suiiste'mol qonuni (CFAA) bo'yicha ayblanishi mumkin. Kompyuter firibgarligi jinoyatlarining oldini olish uchun jismoniy shaxslar va tashkilotlar bir qator chora-tadbirlarni ko'rishlari mumkin, jumladan,

virusga qarshi dasturlardan foydalanish, kuchli parollarni kiritish va fishing hujumlaridan ehtiyot bo'lish. Dasturiy ta'minotni yangilab turish, shuningdek, xakerlar tomonidan ishlatilishi mumkin bo'lgan dasturiy ta'minot zaifliklarining oldini olishga yordam beradi. Xavfsizlikka oid so'nggi tahdidlardan xabardor bo'lib turish hamda o'zingizni va tashkilotingizni himoya qilish uchun choralar ko'rish muhim.

MUHOKAMA

Albatta, kompyuter firibgarligi jinoyati shaxsiy manfaat yo'lida firibgarlik qilish uchun kompyuterlar, internet yoki boshqa raqamli qurilmalardan foydalanishni o'z ichiga olgan kiberjinoyatlarning bir turidir. Kompyuter firibgarligi jinoyatlarining ba'zi keng tarqalgan misollariga identifikatsiyani o'g'irlash, fishing firibgarliklari, to'lovga qarshi hujumlar, zararli dasturlarni infektsiyalari, kredit kartalari bilan firibgarlik va xakerlik kiradi. Kompyuter firibgarligi jinoyati sodir etganlar ko'pincha nozik ma'lumotlar yoki mablag'larga kirish uchun murakkab usullardan foydalanadilar. Ular shaxsiy yoki moliyaviy ma'lumotlarni baham ko'rish uchun shaxslarni aldash uchun ijtimoiy muhandislik taktikalaridan foydalanishlari yoki tizimlar yoki tarmoqlarga ruxsatsiz kirish uchun zararli dasturlardan foydalanishlari mumkin. Raqamli qurilmalardan foydalanishda hushyor bo'lish, ayniqsa, onlayn maxfiy tranzaksiyalarni amalga oshirishda juda muhim. O'zingizni kompyuter firibgarligi jinoyatidan himoya qilishning keng tarqalgan usullariga zamonaviy antivirus dasturlarini o'rnatish, kuchli va noyob parollardan foydalanish, elektron pochta xabarlarini ochish yoki havolalarni bosishda ehtiyot bo'lish va faqat xavfsiz veb-saytlarda tranzaksiyalarni amalga oshirish kiradi.

IDENTIFIKATSIYA O'G'IRLASH

Shaxsni o'g'irlash firibgarlikning bir turi bo'lib, ruxsatsiz xaridlar yoki tranzaksiyalarni amalga oshirish uchun kimningdir shaxsiy ma'lumotlarini o'g'irlashni o'z ichiga oladi. Bu har kim bilan sodir bo'lishi mumkin va ko'pincha jabrlanganlarni moliyaviy va shaxsiy yo'qotishlarga olib keladi. Jinoyatchilar shaxsiy ma'lumotlarni o'g'irlashning bir necha yo'li mavjud. Keng tarqalgan usullardan biri fishing firibgarliklari orqali jinoyatchilar soxta elektron pochta xabarlarini yoki bank yoki davlat idorasi kabi ishonchli manbadan kelganga o'xshash xabarlarini yuborishadi. Bu xabarlarda ko'pincha jismoniy shaxslardan kredit karta ma'lumotlari yoki ijtimoiy xavfsizlik raqamlari kabi shaxsiy ma'lumotlarini kiritishni so'raydigan soxta veb-saytlarga havolalar mavjud. Jinoyatchilar tomonidan qo'llaniladigan yana bir usul bu xakerlik bo'lib, ular shaxsiy ma'lumotlarni o'g'irlash maqsadida kompyuter tizimlari yoki tarmoqlariga ruxsatsiz kirishadi. Bu, ayniqsa, ijtimoiy xavfsizlik raqamlari yoki bank hisobi rekvizitlari kabi nozik ma'lumotlarga nisbatan xavfli bo'lishi mumkin. O'zingizni shaxsingizni o'g'irlashdan himoya qilish uchun hushyor bo'lish va kerakli ehtiyot choralari ko'rish muhim. Bunga kredit karta va bank ko'chirmalarini ruxsatsiz tranzaksiyalar uchun muntazam tekshirish, kuchli va noyob parollardan foydalanish, elektron pochta xabarlarini ochish yoki havolalarni bosishda ehtiyotkor bo'lish va antivirus dasturingizning yangilanganligini ta'minlash kiradi. Bundan tashqari, hisobga kirish uchun parol va tasdiqlash kodini talab qilish orqali qo'shimcha xavfsizlik darajasini ta'minlovchi ikki faktorli autentifikatsiyadan foydalanishni o'ylab ko'ring.

FISHING FIRIBGARLIKLARI

Fishing firibgarliklari elektron aloqada ishonchli shaxs sifatida niqoblanib, jismoniy shaxslardan parollar, kredit karta raqamlari yoki bank hisobi ma'lumotlari kabi maxfiy

ma'lumotlarni olishga qaratilgan firibgarlik harakatlaridir. Ushbu firibgarliklar elektron pochta, matnli xabarlar yoki hatto telefon qo'ng'iroqlari orqali sodir bo'lishi mumkin. Ehtiyot bo'lish va bu turdagi xabarlariga javoban hech qanday havolalarni bosmaslik yoki shaxsiy ma'lumotlarni taqdim qilmaslik muhimdir. To'g'ridan-to'g'ri ishonchli aloqa kanali orqali tashkilotga murojaat qilish orqali har doim shaxsiy ma'lumotlar so'rovlarining haqiqiyligini tekshiring. Firibgarlik qurboni bo'lmaslik uchun hushyor bo'ling va shaxsiy ma'lumotlaringizni himoya qiling.

KREDIT KARTALARI BILAN FIRIBGARLIK

Kredit kartalari bo'yicha firibgarlik xarid qilish yoki naqd pul olish uchun boshqa bironing kredit kartasi yoki kredit karta ma'lumotlaridan ruxsatsiz foydalanishdir. Bu kimdir jismoniy kredit kartasini o'g'irlaganda, fishing firibgarliklari yoki boshqa firibgarlik vositalari orqali kredit karta ma'lumotlarini olganida yoki qonuniy tranzaksiyadan kredit karta ma'lumotlarini o'g'irlash uchun skimming qurilmalaridan foydalanganda sodir bo'lishi mumkin. Agar siz kredit kartangizda firibgarlik harakatiga shubha qilsangiz, muammo haqida xabar berish va firibgarlikni hal qilish jarayonini boshlash uchun darhol bankingiz yoki kredit kartangiz emitentiga murojaat qilishingiz kerak. Kredit kartalar bo'yicha firibgarlikning oldini olish uchun kartangiz ma'lumotlarini xavfsiz saqlash, bank va kredit karta ko'chirmalarini muntazam tekshirib turish va kredit hisobotida ruxsat etilmagan harakatlar mavjudligini kuzatish muhimdir.

XULOSA

Menimcha, kompyuter texnikasidan foydalanish orqali firibgarlik qilish jismoniy shaxslar va tashkilotlar uchun keng qamrovli oqibatlariga olib kelishi mumkin bo'lgan og'ir jinoyatdir. Kundalik hayotimizda texnologiyaga bo'lgan ishonch ortib borayotgan bir paytda, kompyuterga asoslangan firibgarlik holatlarining oldini olish va jinoiy javobgarlikka tortish choralarini ko'rish muhim ahamiyatga ega. Bunga shifrlash va ikki faktorli autentifikatsiya kabi qat'iy xavfsizlik choralarini qo'llash, shuningdek, jismoniy shaxslar va tashkilotlarni firibgarlikni aniqlash va oldini olish bo'yicha o'rgatish kiradi. Bundan tashqari, huquqni muhofaza qilish organlari kelgusida ushbu jinoyat holatlarining oldini olish uchun kompyuterga asoslangan firibgarlik aybdorlarini tergov qilish va jinoiy javobgarlikka tortish uchun faol yondashishi kerak. Umuman olganda, bu masalaga jiddiy yondashishimiz va o'zimizni va jamiyatni kompyuter uskunalar bilan sodir etilgan firibgarlikning salbiy oqibatlaridan himoya qilish uchun birgalikda harakat qilishimiz juda muhim.

References:

1. <https://aniq.uz/uz/yangiliklar/firibgarlik-nima-unga-qanday-jazo-belgilangan>
2. <https://cyberleninka.ru/article/n/axborot-kommunikatsiya-texnologiyalari-sohasida-sodir-etilgan-kiberjinoyatlarning-huquqiy-tavsifi>
3. <https://kun.uz/uz/news/2022/10/20/firibgarlikni-axborot-texnologiyalaridan-foydalanib-sodir-etganlik-uchun-javobgarlik-kuchaytirildi>
4. <https://uz.warbletoncouncil.org/delitos-informaticos-136>
5. <https://www.texnoman.uz/post/internetdagi-firibgarlik-va-qalobliklar.html>
6. <https://civil.uz/firibgarlik-uchun-javobgarlik-qanday/>
7. Abdullayev A.Y., Yolg'on guvohlik berishga oid ayrim masalalar // Siyosatshunoslik,

huquq va xalqaro munosabatlar jurnali. 2022. № 1. C. 60-65.// [https://
https://sciencebox.uz/index.php/siyosatshunoslik/article/view/3916](https://sciencebox.uz/index.php/siyosatshunoslik/article/view/3916)

