INTERNET TARMOG'IDAGI FIRIBGARLIKLAR

D.D. Mirzaakbarov *Farg'ona davlat universiteti axborot texnologiyalari kafedrasi o'qituvchisi*
M.O. Urazova
Far'ona Davlat Universiteti iqtisodiyot fakulteti Moliya moliyaviy texnalogiyalar yo'nalishi 1-bosqich talabasi

Kalit so'zlar: *tarmoq, raqamli iqtisodiyot, sanoat inqilobi, xavfsizlik, firibgarlik, dastur.*

Ключевые слова: *сеть, цифровая экономика, индустриальная революция, мошенничество, прагрома.*

Keywords: *network, digital economy, the industrial revolution, fraud, programm.*

Anotatsiya.

Tarmoq firibgarligi bugungi raqamli iqtisodiyotda jiddiy tashvish tug'diradi, bu jismoniy shaxslar, korxonalar va umumiy iqtisodiy manzaraga keng ko'lamli ta'sir ko'rsatadi. Ushbu turdagi firibgarlik keng qamrovli noqonuniy faoliyatni, jumladan, shaxsiy ma'lumotlarni o'g'irlash, fishing, to'lov dasturi hujumlari va onlayn firibgarlikning turli shakllarini o'z ichiga oladi. Tarmoq firibgarligining keng tarqalgan tabiati global iqtisodiyotning o'zaro bog'liqligi, shuningdek, moliyaviy operatsiyalarni amalga oshirish va maxfiy ma'lumotlarni saqlash uchun raqamli texnologiyalarga tobora ortib borayotgan bog'liqlikning mahsulotidir.

Сетевое мошенничество является серьезной проблемой в современной цифровой экономике, имеющей далеко идущие последствия для отдельных лиц, предприятий и всей экономической ситуации. Этот тип мошенничества включает в себя широкий спектр незаконных действий, включая кражу личных данных, фишинг, атаки программ-вымогателей и различные формы онлайн-мошенничества. Распространенный характер сетевого мошенничества является результатом взаимосвязанности глобальной экономики, а также растущей зависимости от цифровых технологий для проведения финансовых транзакций и хранения конфиденциальной информации.

Network fraud is a serious concern in today's digital economy, with far-reaching effects on individuals, businesses, and the overall economic landscape. This type of fraud involves a wide range of illegal activities, including identity theft, phishing, ransomware attacks, and various forms of online fraud. The pervasive nature of network fraud is a product of the interconnectedness of the global economy, as well as the growing reliance on digital technologies to conduct financial transactions and store sensitive information.

Onlayn firibgarlik (yoki internetdagi firibgarlik) Internet orqali va elektron pochta orqali sodir bo'ladigan turli xil firibgarlik turlarini anglatadi—masalan, shaxsni o'g'irlash, fishing, hisobni egallash va hokazolar.

Onlayn firibgarlik individual iste'molchilardan tortib yirik korxonalar va texnologik kompaniyalargacha bo'lgan hamma uchun jiddiy muammodir. COVID-19 dan oldin ham "raqamli transformatsiya" va "sanoat inqilobi 4.0" (internet tomonidan quvvatlanadi) mashhur so'zlar edi. Keyinchalik, global pandemiya butun dunyo bo'ylab turli sohalarda raqamli o'zgarishlarni tezlashtirdi. Afsuski, onlayn faoliyatning ko'payishi, ayniqsa, onlayn operatsiyalar, ko'plab kiber jinoyatchilarni turli xil hujumlarni amalga oshirishga imkoniyat tug’dirdi. FQBning 2021 yildagi Internet tizimidagidagi jinoyatlar to'g'risidagi hisobotiga ko'ra, 800,000 onlayn firibgarlik bilan bog'liq shikoyatlar bo'lgan. Xabar qilingan uchta jinoyat fishing, elektron tijorat operatsiyalarida etkazib bermaslik, to'lamaslik firibgarligi va onlayn tovlamachilik edi.

Ushbu maqolada onlayn firibgarlik va boshqa turdagi kiberhujum vektorlari, ayniqsa, raqamli aktivlaringizni firibgarlikdan qanday himoya qilish haqida, ko’pchilik bilishi kerak bo'lgan barcha narsalarni qamrab olish maqsadida so’z yuritamiz. Dastlab quydigailarni aniqlab olaylik;

- **Onlayn firibgarlik nima?**
- **Onlayn firibgarlikning har xil turlari xaqiada bilasizmi?**
- **O'zingizni va raqamli aktivlaringizni onlayn firibgarlikdan qanday himoya qilish kerak?**

Onlayn firibgarlik-bu Internet yordamida sodir etilgan har xil firibgarliklarni qamrab olish uchun soyabon atamasi. Onlayn firibgarlikni amalga oshiruvchilar turli xil shakllarda va turli xil tajovuzkorlar xar xil g’arazli maqsadlarni ko'zlaydilar. Masalan, tajovuzkor fishing- bu elektron pochta xabarlarini, ya’ni shaxsiy foydalanuvchi ma'lumotlarini olish va boshqa maqsadlar uchun hisob ma'lumotlarini to'ldirish hujumidan foydalanadi.

Eng onlayn firibgarlikni olsak – bu o'g'irlanish yoki moliyaviy firibgarlikni ham o'z ichiga oladi. Shaxsni o'g'irlash jabrlanuvchining shaxsiy jinoyatini amalga oshirish yoki unga yordam berish uchun (jabrlanuvchining bilimisizligidan) foydalanilganda sodir bo'ladi. Moliyaviy firibgarlik, nomidan ko'rinib turibdiki, tajovuzkor firibgarlik bilan pul daromadini jabrlanuvchidan oladiga firibgarlikning bir turi hisoblanadi. Shaxsni o'g'irlash va moliyaviy firibgarlik jinoyatlari bilan bog'liq bo'lishi mumkin. Masalan, kiberjinoyatchi iste'molchining kredit karta ma'lumotlariga kirish huquqiga ega bo'lishi va keyin kredit yoki kredit kartadandan foydalangan holda o'zini iste'molchi sifatida ko'rsatishi mumkin.

Onlayn firibgarlik turli shakllarda bo'lishi mumkin bo'lsa-da, bu yerda eng mashhurlari:

Tibbiy shaxsni o'g'irlashdir.

Hujumchilar tibbiy sug'urta ma'lumotlariga ruhsatsiz kirishlari mumkin, so'ngra qurbonlarning ma'lumotlarini retsept bo'yicha dori-darmonlarni olishi, sug'urta provayderlariga noqonuniy da'volar qilishi va hokazolar aldovlarni amalga oshirishi mumkin. Tibbiy shaxsni o'g'irlashning oldini olish uchun bemorlar sug'urta va tibbiy bayonotlarni iloji boricha muntazam ravishda, diqqat bilan ko'rib chiqishlari kerak. Agar shaxs o'z yozuvlariga ruhsatsiz begona shaxslar tomonidan kirganiga shubha qilsa, ular darhol tafsilotlarni o'zaro tekshirish uchun sog'liqni saqlash tashkilotining mijozlarga xizmatiga qo'ng'iroq qilishlari kerak bo'ladi.

Tibbiy va sug'urta provayderlarini imkon qadar, tezroq buzilish va o'zgarish haqida gohlantirish muhimdir. Bemorlar o'zlarining nizolarini asoslash uchun tasdiqlovchi hujjatlarni taqdim etishga tayyor bo'lishlari lozim bo'ladi. Shikoyat berilgandan so'ng, tergov jarayoni biroz vaqt talab qilishi mumkin, shuning uchun hamma narsa aniq ekanligiga ishonch hosil qilish uchun jarayonni kuzatib boorish lozim bo'ladi.

Ijtimoiy Tarmoqlarda Shaxsni O'g'irlash.

Dunyo bo'ylab ijtimoiy media foydalanuvchilarining ko'payishi bilan ko'plab kiberjinoyatchilar hozirda turli xil firibgarlik maqsadlarida ijtimoiy media akkauntlarini nishonga olishmoqda. Kiberjinoyatchilar turli xil shakllar orqali ijtimoiy tarmoqlardagi akkauntlarga kirishga harakat qilishlari mumkin bu hisobni egallash (ATO) firibgarligidir. Kirish imkoni bo'lmaganda ham, tajovuzkorlar foydalanuvchilarning postlaridagi ma'lumotlaridan firibgarlik maqsadida foydalanishlari mumkin. Misol uchun, agar foydalanuvchi Instagramda o'z uyining rasmini joylashtirgan bo'lsa, bu rasm orqali kiberjinoyatchi manzilni kuzatishi va undan kredit karta olish uchun foydalanishi turgan gap..

Ijtimoiy tarmoqlarda shaxsni o'g'irlashning oldini olish uchun foydalanuvchilar o'z xavfsizligini ta'minlash uchun ishlatilishi mumkin bo'lgan narsalarni joylashtirishdan oldin juda ehtiyot bo'lishlari kerak. Ijtimoiy media foydalanuvchilari, shuningdek, ular bilmagan foydalanuvchilarning ulanish takliflarini rad etishlari kerak bo'ladi.

Ijtimoiy Xavfsizlik Raqami O'g'irlanishi.

Ijtimoiy xavfsizlik ma'lumotlarini himoya qilish sog'lom fikr kabi ko'rinishi mumkin. Ammo ko'p odamlar tajovuzkorlar ijtimoiy sug'urta raqamiga kirish huquqiga ega bo'lgach, ular soliq yozuvlariga ham kirishlari mumkinligini bilishmaydi, keyinchalik ular turli xil moliyaviy firibgarlik urinishlarini boshlash uchun ishlatilishi mumkin.

Fishing.

Fishing hujumida kiberjinoyatchilar maxfiy ma'lumotlarni (masalan, foydalanuvchi nomi, parol ma'lumotlari, kredit karta ma'lumotlari va ijtimoiy xavfsizlik raqami) olish uchun ijtimoiy muhandislik taktikasidan foydalanadilar. Fishing hujumlari turli xil shakllarda bo'lishi mumkin, masalan: Elektron pochta orqali

Fishing firibgarligi: kiberjinoyatchi foydalanuvchilarga ma'lum bir shaxsni (masalan, bank) taqlid qilib elektron pochta xabarlarini yuboradi va qurbonlarni biror narsani yuklab olishga yoki havolani bosishga olib keladi. Havola yoki yuklab olish jabrlanuvchining ma'lumotlarini o'g'irlaydi yoki jabrlanuvchining qurilmasiga zararli dasturni yuklaydi.

Nayza Fishing.

Ma'lum bir shaxsni masalan, yirik kompaniya(KIA)ning nishonga olish uchun tajovuzkor tadqiqot olib boradi va keyin jabrlanuvchi biladigan odamni taqlid qiladi (masalan, bosh direktor, uning haqiqiy ismi va telefon raqamidan foydalangan holda). Soxta hotspotni ushlash: tajovuzkorlar Fishing tarmog'iga ulangan qurbonlarning ma'lumotlarini ushlab turadigan soxta hotspot (bu bepul) yaratishi mumkin.

Uyda ishlash firibgarligi.

Pandemiyadan keyingi davrda kiberjinoyatchilar qurbonlarni (haqiqiy ish ovchilari) uydan ishlash imkoniyatlarini chegaralash fishingning juda keng tarqalgan shaklidir. Fishingdan himoya qilish qiyin, chunki u odamlarga qaratilgan. Xavfsizlik infratuzilmangiz qanchalik mustahkam bo'lmasin, tashkilotingizning fishing himoyasi sizning eng hushyor xodimingiz kabi kuchlidir.

Hisob-Fakturadagi Firibgarlik.

Hisob-fakturadagi firibgarlikda kiberjinoyatchi biznesni (yoki maqsadga hisob-fakturani yuborishi mumkin bo'lgan har qanday tomonni) taqlid qiladi va haqiqiy sotuvchi tomonidan yuborilgan schyot-fakturalar uchun bank ma'lumotlarini yangilashni so'rab, elektron pochta yoki boshqa tarmoq vositalari orqali qandaydir maqsad bilan bog'lanadi. Keyin, to'lovlar amalga oshiriladi. Agar tajovuzkor etkazib beruvchi-sotuvchining fonida etarlicha tadqiqot o'tkazgan bo'lsa, hisob-fakturadagi firibgarlikni aniqlash juda qiyin bo'lishi mumkin, chunki so'rov juda haqiqiy ko'rinishi mumkin.

Elektron tijorat onlayn xaridlar veb-saytidagi Firibgarlik.

Bugungi kunda elektron tijorat firibgarligi juda keng tarqalgan. Hujumchilar odatda yuqori talabga ega mahsulotlarni (iPhone, Samsung, VGA kartalari, PS5 va boshqalar) taklif qiladigan soxta onlayn xarid qilish saytini o'rnatdilar) juda arzon narxlarda taklif qiladilar. Soxta veb-sayt ko'plab potentsial qurbonlarni jalb qilishi va ularni kredit karta ma'lumotlarini kiritish orqali sotib olishga undashi uchun mo'ljallangan bo’ladi. Afsuski, qurbonlar hech qachon mahsulotni olmaydilar va jinoyatchi pul va kredit karta ma'lumotlarini oladi. Triangulyatsiya firibgarligi deb nomlangan modifikatsiya ham mavjud, bu erda tajovuzkor soxta elektron tijorat saytidan olgan kredit karta ma'lumotlarini qonuniy saytdan haqiqiy mahsulotni sotib olish uchun ishlatadi. Shunday qilib, jabrlanuvchi haqiqiy mahsulotni oladi va kredit karta ma'lumotlari buzilganligini tushunmaydi. Triangulyatsiya firibgarligi

tajovuzkorlarga blokirovka qilinishidan oldin o'g'irlangan kredit karta ma'lumotlaridan foydalanish uchun ko'proq vaqt sotib oladi.

Lotereya Firibgarligi.

Odamlar hali ham qurboniga aylanadigan onlayn firibgarlikning nisbatan "eski" turi bu lotereya firibgarligi. Jabrlanuvchi lotereya yutganligi to'g'risida bildirishnoma elektron pochta orqali matn oladi (pul yoki iPhone, noutbuk, bepul chiptalar va boshqalar kabi boshqa foydali sovg'alar). Ammo jinoyatchi jabrlanuvchidan o'z mukofotini talab qilish uchun haq to'lashini so'raydi. Masalan, tajovuzkor jabrlanuvchidan soliqlar, sug'urta xarajatlari, kurerlik to'lovlari va hokazolarni to'lashni so'rashi mumkin. Jabrlanuvchi to'lovlarni amalga oshiradi va firibgar tuzog'iga ilinadi.

Xulosa qilib aytadigan bo'lsak, tarmoqdagi firibgarlik jismoniy shaxslarga, biznesga va kengroq iqtisodiyotga ta'sir ko'rsatadigan raqamli asrda muhim iqtisodiy muammolarni keltirib chiqaradi. Firibgarlik faoliyatining ko'payishi bevosita moliyaviy yo'qotishlarga olib kelishi, iste'molchilar ishonchini yo'qotishi va raqamli iqtisodiyotning ishlashi uchun zarur bo'lgan ishonchni susaytirishi mumkin. Ushbu muammolarni hal qilish texnologik innovatsiyalar, tartibga soluvchi nazorat va faol ta'lim va xabardorlik tashabbuslarini o'z ichiga olgan muvofiqlashtirilgan sa'y-harakatlarni talab qiladi. Tarmoq firibgarligiga qarshi birgalikda kurashish orqali jismoniy shaxslar, korxonalar va siyosatchilar hamma uchun xavfsizroq va farovon raqamli iqtisodiyotni yaratishga yordam berishlari mumkin.

Foydalanilgan Adabiyotlar.

1. Nigmatov X., Tursunov N. Axborot xavfsizligi. O'quv qo'llanma. "Toshkent islom universiteti nashriot-matbaa birlashmasi" nashriyoti. Toshkent shaxri. 2018 й.120 bet.
2. Mirzaakbarov D.D., Ismoilova D.S. "Oliy ta'lim muassasalarida bulutli texnologiyalardan foydalanish metodikasi" Qaraqalpaqstan Baspa səz həm xabar agentligi tarepinen, 4/2-san 2023 iyul.Nukus.
3. Muzaffarxonov Saida'loxon, Mirzaakbarov Dilshodbek Dovlatboyevich "Sun'uy Intelekt
4. Yordamida Pochta Xizmatini Tashkil Qilish" Miasto Przyszłości Kielce 2023.