Impact Factor: 9.9 ISSN-L: 2544-980X

Axborot Va Kiberxavfsizlik Sohasida Ijtimoiy Muhandislik

Urimbetova Zinaxan Abdirazakovna [1]

Annotatsiya: Ushbu maqolada ijtimoiy muhandislik va fishingdan himoyalanishning asosiy usullari muhokama qilingan, hozirgi kiberxavfsizlik tahdidlari sharoitida ularning afzalliklari va kamchiliklari tahlil qilingan. Unda hujumlarni oldini olishning texnik va xulq-atvor yondashuvlari, jumladan, foydalanuvchilarni o‘qitish, autentifikatsiya mexanizmlari, antivirus dasturlaridan foydalanish va boshqalar ko‘rib chiqiladi. Muallif o‘quvchilarga zamonaviy raqamli texnologiyalar dunyosida ijtimoiy muhandislik va fishingning jiddiy oqibatlarini oldini olishga yordam beradigan samarali himoya usullarini chuqurroq tushunishni taklif qiladi.

Kalit so‘zlar: fishing, smishing, ijtimoiy muhandislik, axborot, usul, hujumkor, preteksting.

Dolzarblik. Zamonaviy insonni aqlli gadjetlar, internet tarmog‘i va boshqa axborot-kommunikatsiya texnologiyalaridan foydalanmasdan tasavvur qilish qiyin. Vaqt bilan hamnafas bo‘lishga harakat qilib, biz beixtiyor virtual reallikka sho‘ng‘ib ketamiz, internet firibgarlariga o‘zlari uchun zarur bo‘lgan har qanday ma’lumotni olishlariga imkon beramiz. Ular orasida ijtimoiy muhandislik va fishing tashkilotlarning tizimlari va ma’lumotlar bazalariga kirishning eng samarali va xavfli usullaridan biri sifatida ajralib turadi.

O‘zbekiston Respublikasining "Axborotlashtirish to‘g‘risida"gi Qonuniga muvofiq, axborot resurslari, axborot texnologiyalari va axborot tizimlaridan foydalangan holda yuridik va jismoniy shaxslarning axborotga bo‘lgan ehtiyojlarini qondirish uchun shart-sharoitlar yaratishning tashkiliy ijtimoiy-iqtisodiy va ilmiy-texnikaviy jarayoni hisoblanadi[1].

Internet tarmog‘idan va boshqa axborot-kommunikatsiya vositalaridan zamonaviy foydalanuvchi uchun asosiy tahdidlardan biri ijtimoiy muhandislik- axborot xavfsizligi kontekstida zamonaviy tushuncha hisoblanadi.

Mazkur holatda ijtimoiy injeneriyani ma’lumotlarni to‘plash, tahlil qilish va uni jinoyatchilar tomonidan ma’lum bir shaxsga qarshi g‘arazli maqsadlarda, ishontirish, manipulyatsiya qilish va boshqalar orqali foydalanish sifatida tavsiflash mumkin. Bunday axborotni to‘plashning pirovard maqsadi jabrlanuvchilar ixtiyoridagi pul mablag‘lari va boshqa ma’lumotlarni g‘ayriqonuniy ravishda olishdir.

Tadqiqot maqsadi. Ijtimoiy muhandislikdan foydalangan firibgarlik operatsiyalari turli xil bo‘ladi. Shuning uchun ijtimoiy muhandislik nima ekanligini va u qanday ishlashini tushunish muhimdir. Asosiy mexanizmini anqlashni o‘rganib, siz o‘zingizni va yaqinlaringizni firibgarlardan himoya qilishingiz mumkin.

Firibgarlarning odamlarga manipulyatsion ta’sir ko‘rsatish orqali kompaniyalar ishiga aralashuvi ma’lumotlarning maxfiyligi va yaxlitligini xavf ostiga qo‘yadi, shuningdek, tashkilotlar uchun moliyaviy va obro‘li xavflarni keltirib chiqaradi. Ijtimoiy muhandislik - bu tajovuzkorning texnik vositalardan foydalanmasdan kerakli ma'lumotlarni olish yoki inson harakatlarini nazorat qilish usuli. Ijtimoiy muhandislikning mohiyati odamlarga ta'sir qilishda ishontirish, ishonchga kirish va ayyorlik kabi psixologik usullaridan foydalanishdir.

Fishing - bu foydalanuvchilarning maxfiy ma’lumotlari- login va parollarga kirish uchun mo‘ljallangan Internet firibgarligining bir turi. Bunga mashhur brendlar nomidan ommaviy elektron

[1] Assistent o’qituvchisi, Qoraqalpoq davlat universiteti “Amaliy matematika va informatika” kafedrasi

pochta xabarlarini, shuningdek, turli xizmatlar ichida, masalan, banklar nomidan yoki ijtimoiy tarmoqlar ichida shaxsiy xabarlarni yuborish orqali erishiladi. Xatda ko‘pincha tashqi tomondan haqiqiydan farq qilmaydigan saytga yoki redirektli saytga to‘g‘ridan-to‘g‘ri havola mavjud. Foydalanuvchi soxta sahifaga kirgandan so‘ng, firibgarlar turli xil psixologik usullar bilan uni soxta sahifaga o‘zining login va parolini kiritishga undashga harakat qilishadi, u ma’lum bir saytga kirish uchun foydalanadi, bu esa firibgarlarga hisoblar va bank hisoblariga kirish imkonini beradi[2].

Fishing - bu kiberhujum usuli bo‘lib, unda jinoyatchi maxfiy ma'lumotlarni tortib olish uchun jabrlanuvchining ishonchini qozonishga urinadi. Shuningdek firibgarlar, ma'lumotlarni olish uchun shoshilinchlik hissi yaratadilar yoki qo‘rqitish taktikalaridan foydalanadilar. Fishing hujumida siz ishonchliday ko‘rinadigan manbadan ma'lumotlaringiz so‘ralgan elektron pochta yoki xabar olasiz. Fishing foydalanuvchilarning tarmoq xavfsizligi asoslarini bilmasligiga asoslangan ijtimoiy muhandislikning bir turi. Xususan, ko‘pchilik oddiy faktni bilmaydi: servislar o‘zlarining hisob ma’lumotlari, parollari va boshqalarni berishlarini so‘rab xatlar yubormaydi. Elektron xatlar, messenjerlardagi xabarlar va soxta saytlar yordamida firibgarlik qilish klassik fishing hisoblanadi. Vaqt o‘tishi bilan fishing uchun boshqa aloqa usullari ham qo‘llanila boshlandi: masalan, telefon va sms. Ushbu fishing turlari uchun hatto alohida atamalar - "vishing" va "smitching" paydo bo‘ldi.

Smishing (SMS-fishing yoki smishing) - qisqa telefon xabaridan foydalanish orqali kiberfiribgarlik hujumi. Amal qilish printsipi elektron pochta orqali fishing hujumlarini amalga oshirish bilan bir xil: buzg‘unchi qonuniy deb hisoblangan jo‘natuvchidan (masalan, ishonchli kompaniyadan) zararli havolasini o‘z ichiga olgan matnli xabarni jo‘natadi.

Havola kupon kodi (keyingi buyurtmangizga 20% chegirma) yoki konsert chiptasiga o‘xshash narsani yutib olish taklifi bilan niqoblanishi mumkin. Tabiiyki, bunday havola orqali o‘tgandan so‘ng, ehtimoliy jabrlanuvchini yoqimsiz syurprizlar kutadi. Shunday qilib, biz ijtimoiy injiniringni tarqatish va undan foydalanish oddiy foydalanuvchilar uchun xavf tug‘dirishini ko‘ramiz, ularning hushyorligi va ehtiyotkorligi hatto eng zamonaviy tahdidlarga ham qarshi tura oladi.

Statistik ma’lumotlarga ko‘ra, fishing hali ham elektron pochtaga hujum qilishning eng keng tarqalgan usuli bo‘lib qolmoqda, barcha elektron pochta tahdidlarining 39,6 foizi uning hissasiga to‘g‘ri keladi. Zararli dasturlarning 94 foizi elektron pochta (Panda) orqali yetkazib beriladi. Fishing hujumlarining 62% da fishing investitsiyalari ishlatilgan, 33% da havolalar va 5% da xizmat sifatida foydalanilgan (IBM Security X-Force 2023). 2022-yilda kredit kartalari haqidagi ma’lumotlardan faqat 29% fishing to‘plamlarida foydalanilgan, bu 2021-yilga nisbatan 52% ga kam (IBM Security X-Force 2023). Ko‘pincha fishing havolalari bilan bog‘liq bo‘lgan ishbilarmonlik elektron pochtasi (BEC) ni obro‘sizlantirish 6% hodisalarni tashkil etdi va bu holatlarning yarmida fishing havolalari ishlatilgan boz ustiga, ushbu holatlarning yarmida fishing havolalari ishlatilgan (IBM Security X-Force 2023). BEC hujumi sodir bo‘lgan tashkilotlarning 80 foizida hodisadan oldin ko‘p omilli autentifikatsiya ("MFA") (ArcticWolf) uchun yechim yo‘q edi. Fishing kiberxavfsizlik hodisalarining 41 foizida asosiy infeksiya tashuvchisi sifatida aniqlangan (IBM Security X-Force 2023). Oqimlarni ushlab qolishga urinishlar soni 2022-yilda 2021-yilga nisbatan ikki baravar ko‘paydi (IBM Security X-Force 2023).

Ijtimoiy muhandislik - bu texnik vositalardan foydalanmasdan ma’lumot yoki ma’lumotlarni saqlash tizimlariga ruxsatsiz kirish usuli (hujum). Ijtimoiy muhandislik – bu odamlarga ruhiy yoki ijtimoiy ta'sir o'tkazish yo'li bilan ularning maxfiy yoki shaxsiy ma'lumotlarini olishga urinish jarayoni. Bu usulda kiberjinoyatchilar turli manipulyatsiyalar orqali odamlarni aldashadi yoki ishonchiga kiradilar. Ijtimoiy muhandislik texnikalari qatoriga phishing (elektron xabar orqali aldash), shaxsiy suhbatlar, telefon qo'ng'iroqlari va boshqa usullar kiradi. Maqsad – odamlardan o'z ixtiyori bilan ularning ma'lumotlarini olish yoki ularni tashkilotning ichki tizimlariga kirish uchun aldashdir.Usul insonning kamchiliklari - inson omilidan foydalanishga asoslangan va juda samarali hisoblanadi[3].

Qarshilik ko‘rsatuvchi zarba obyekti xodimlari haqidagi ma’lumotlarni oddiy telefon qo‘ng‘irog‘i orqali yoki tashkilot xodimi sifatida kirib, axborot to‘plash orqali olishi mumkin[4].

Tadqiqot manbay va usullari. Ijtimoiy muhandislikning barcha texnikasi insonlarning qaror qabul qilish xususiyatlariga asoslanadi. Preteksting - oldindan tuzilgan ssenariy (pretikst) bo‘yicha ishlab

chiqilgan harakat. Natijada, nishon (qurbon) ma’lum bir ma’lumotni berishi yoki ma’lum bir harakatni amalga oshirishi kerak. Bu hujum turi odatda telefonda qo‘llaniladi.

Ko‘pincha bu usul shunchaki yolg‘ondan ko‘ra ko‘proq narsani o‘z ichiga oladi va qandaydir dastlabki tadqiqotlarni talab qiladi (masalan Personalizatsiya: xodimning ismini, egallab turgan lavozimini va u ishlayotgan loyihalarning nomlarini aniqlash), maqsadning ishonchliligini ta’minlash uchun. Troya oti: bu texnika maqsadning qiziquvchanligi yoki ochko‘zligidan foydalanadi. Firibgar ilovaga antivirusning muhim yangilanishi yoki hatto xodimga nisbatan yangi ma’lumot kiritilgan e-pochtani yuboradi. Bunday texnika foydalanuvchilar har qanday investitsiyaga ko‘r-ko‘rona qo‘ng‘iroq qilgunlaricha samarali bo‘lib qoladi. Yo‘l olmasi: bu hujum usuli troyan otining moslashuvidir va jismoniy tashuvchilardan foydalanishdan iborat. Firibgar zararlangan CD yoki xotira kartasini joy, hududga tashlashi mumkin. Agar ular mavjud bo‘lsa, ularni "yechish" jarayonida nishon buzg‘unchiga zararli dasturiy ta’minotni ishga tushirishga imkon beradigan buyruqlarni kiritadi.Teskari ijtimoiy muhandislikning maqsadi maqsadning o‘zini yovuz niyatli shaxsga "yordam" so‘rab murojaat qilishga majbur qilishdir. Jabrlanuvchining o‘zi jinoyatchiga kerakli ma’lumotni taklif qilganda, teskari ijtimoiy muhandislik haqida eslatib o‘tiladi: "Sen - menga, men - senga." Halol ayirboshlash talonchilik emas, deyishadi, lekin bu holda emas. Ko‘pgina ijtimoiy muhandislar o‘z qurbonlarini ma’lumotlar evaziga nimadir olishlariga yoki ulardan foydalanishlariga ishontirishadi. Foydalanuvchiga uning kompyuteridagi tahdidni yo‘q qilishni taklif qiluvchi soxta antivirus shunday ishlaydi, garchi "antivirus"ning o‘zi tahdid bo‘lsa ham. Elektron pochtani buzish va kontaktlar bo‘yicha tarqatish. Firibgar shaxsning pochtasini yoki ijtimoiy tarmoqdagi akkauntini buzib, uning kontaktlariga kirishga muvaffaq bo‘ladi. Endi jabrlanuvchi nomidan u o‘g‘irlanganini xabar qilishi va pul o‘tkazishni yoki zararli dasturiy ta’minot yoki klaviatura josusiga qiziq video niqobi ostida havola yuborishni so‘rashi mumkin [5].

Odatda, aloqa qilishdan oldin, firibgarlar ma'lumotlar bazalarini buzish orqali odamlar haqida maxfiy ma'lumotlarni olishga harakat qilishadi. Ba'zan odamlarning o‘zlari ijtimoiy tarmoqlarda telefon raqamlari, elektron pochta manzillarini joylashtirishadi / ko‘rsatishadi va hatto shaxsni tasdiqlovchi hujjatlar va bank kartalarining fotosuratlarini ham yuklaydilar. Albatta bu ma'lumotlar pulni o‘g‘irlash uchun yetarli emas, lekin ulardan suhbat davomida foydalanish mumkin. Firibgarlar odamlarga ism va familiyalari bilan murojaat qilganda, sizni o‘zlarining haqiqatan ham tashkilot xodimlari ekanligiga ishontirish uchun sizga tegishli bo‘lgan karta raqami yoki boshqa maxfiy ma'lumotlarni o‘zlari aytishadi.

Firibgarlar oson pul topish vadalari bilan o‘ziga tortadi – ular odamlarning oson boyib ketish istagidan faol foydalanadilar. Ular katta miqdordagi yutuqlar mavjud bo‘lgan maxsus saytlar yaratadilar. Masalan, ular pul mukofoti evaziga so‘rovnomada qatnashishni yoki "yutqizmaslik" shartlari asosida tanlovlarda qatnashishni taklif qilishadi. Ushbu firibgar saytlar ijtimoiy tarmoqlarda reklama qilinadi, SMS va messenjerlar orqali yuboriladi.

Tadqiqot natijalari. Ijtimoiy muhandislikdan himoyalanishning texnik usullari maxfiy ma’lumotlarni olish uchun manipulyatsiya va aldashdan foydalanadigan jinoyatchilarning hujumlarini oldini olishga qaratilgan turli chora-tadbirlar va texnologiyalarni o‘z ichiga oladi. Quyida ijtimoiy muhandislikdan himoyalanishning asosiy texnik usullari keltirilgan:

1. Ko‘p omilli autentifikatsiyadan foydalanish
2. Monitoring va audit tizimlarini o‘rnatish
3. Ma’lumotlarni shifrlash
4. Himoya dasturiy ta’minotini o‘rnatish
5. Muntazam yangilash va xizmat ko‘rsatish

Ijtimoiy muhandislik va fishing bilan kurashishning mavjud usullarini o‘rganib, ularning har birining o‘ziga xos afzalliklari va kamchiliklari borligini va ularni to‘laqonli tahlil qilish uchun ularni ko‘rib

chiqish kerakligini aniq tushunish kerak[6]. Mavjud usullarning afzalliklariga quyidagi xususiyatlarni aniq kiritish mumkin:

a) xodimlarning hujum usullari haqida xabardorligini oshirish va ularning potensial xavfli vaziyatlarni aniqlash ko‘nikmalarini mustahkamlash;

b) kompyuterlar va tarmoqlarni zararli dasturlardan himoya qilish, bu ma’lumotlarning yuqishi va sizib chiqishi xavfini kamaytiradi;

v) ko‘p fakturali autentifikatsiya orqali tizimga kirish uchun qo‘shimcha ma’lumotlarni kiritishni talab qilish orqali qo‘shimcha xavfsizlik darajasini ta’minlash;

g) xavfsizlik tizimlaridagi zaiflik va muammolarni aniqlash, bu o‘z vaqtida tuzatish choralarini ko‘rish imkonini beradi;

d) maxfiy ma’lumotlarni ruxsatsiz foydalanishdan himoya qilish va axborotni shifrlash, bu uni uchinchi shaxslar uchun tushunarsiz qiladi.

e) xodimlar uchun ijtimoiy muhandislik va fishingdan kelishilgan va samarali himoyani ta’minlashga yordam beradigan aniq qoidalar va tartiblarni yaratish.

Mavjud usullarning afzalliklari haqiqatan ham ko‘p, lekin, ehtimol, hammasini boshqa tomondan ko‘rib chiqamiz.

Garchi fishing va ijtimoiy muhandislikdan himoyalanishning turli usullari mavjud bo‘lsa-da, ular kamchilik va kamchiliklardan xoli emas. Mana ulardan ba’zilari:

1) foydalanuvchilarning yetarli darajada xabardor emasligi;

2) hujumning yangi usullarini aniqlashning murakkabligi;

3) himoyalanish darajasining beqarorligi;

4) xavfsizlik va foydalanish qulayligini muvozanatlashning murakkabligi;

5) turli himoya usullarining yetarli darajada integratsiyalashmaganligi;

6) mobil qurilmalarning yetarli darajada himoyalanmaganligi;

7) himoyaning dolzarbligini saqlashning murakkabligi;

8) bulutdagi axborotni himoyalash muammolari;

9) xavfsizlik bo‘limlari o‘rtasida yetarli darajada muvofiqlashtirilmagan [7].

Xulosa qilib aytganda, ijtimoiy muhandislik va fishingdan himoyalanishning bir qator samarali usullari mavjud bo‘lib, ular firibgarlar tuzog‘iga tushish xavfini sezilarli darajada kamaytirishi mumkin. Biroq ularning har biri o‘ziga xos afzallik va kamchiliklarga ega. Masalan, xodimlarni firibgarlik belgilariga o‘rgatish va muntazam treninglar o‘tkazish xodimlarning xabardorlik darajasini oshirishi mumkin, ammo vaqt talab qiladi. Antiviruslar va spam filtrlaridan foydalanish kabi texnik choralar zararli dasturiy ta’minotdan yaxshi himoyani ta’minlaydi, ammo har doim ham ilg‘or hujumlarga qarshi samarali emas.

Shunday qilib, ijtimoiy muhandislik va fishingdan himoyalanishning optimal strategiyasi inson omilini ham, texnik jihatlarni ham hisobga oluvchi turli xil usullarning kombinatsiyasini o‘z ichiga oladi. Axborot va shaxsiy ma’lumotlar xavfsizligini ta’minlash uchun o‘z bilimlarini doimiy ravishda oshirib borish va eng yangi texnologiyalarni qo‘llash muhimdir.

Foydalanilgan adabiyotlar ro’yxati:

1. O‘zbekiston Respublikasining qonuni, 11.12.2003 yil. 560-II-son
2. Фишинг: что это и как его распознать [сайт].-URL: https://journal.tinkoff.ru/phishing/?ysclid=ltlzwp0iec124574853

3. Социальная инженерия – защита и предотвращение // Блог Касперского [сайт]. – URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-socialengineering-attacks?ysclid
4. Краткое введение в социальную инженерию [сайт]. – URL: https://habr.com/ru/articles/83415/
5. Социальная инженерия: её техники и методы защиты [сайт]. – URL: https://scilead.ru/article/3646-sotsialnaya-inzheneriya-ee-tekhniki-i-metodi.
6. Максименко, Р. О. Типовой алгоритм воздействия в социальной инженерии/ Р. О. Максименко //Интерэкспо Гео-Сибирь. – 2019. – Том 6. – № 2.– С. 33–38.
7. Тепляков, С. П. Социальная инженерия: анализ и методы защиты / С. П. Тепляков // Academy. – 2018. – № 7 (34). – С. 26–27.