AXBOROT XAVFSIZLIGIDAGI ZAMONAVIY TAHDIDLAR: FISHING VA IJTIMOIY MUHANDISLIK HUJUMLARI

Alayev S.R, Mahmudov Sh.T.

Annotatsiya: Ushbu maqolada fishing va ijtimoiy muhandislik hujumlarining axborot xavfsizligiga tahdidi tahlil qilinadi. Ushbu tahdidlar texnologik vositalardan tashqari, inson psixologiyasidan foydalanishga asoslanadi. Maqolada hujumlarning asosiy turlari, real misollar va ularni oldini olish yo‘llari keltirilgan.

Kalit so‘zlar: Fishing, ijtimoiy muhandislik, axborot xavfsizligi, kiberhujum, psixologik tahdidlar.

Аннотация: В данной статье анализируются угрозы информационной безопасности, связанные с фишингом и атаками социальной инженерии. Эти угрозы основаны не только на технических средствах, но и на использовании человеческой психологии. Представлены основные виды атак, реальные примеры и меры профилактики.

Ключевые слова: Фишинг, социальная инженерия, информационная безопасность, кибератака, психологические угрозы.

Abstract: This article analyzes the threats to information security posed by phishing and social engineering attacks. These threats are based not only on technical tools but also on the manipulation of human psychology. The paper presents main types of attacks, real-life examples, and prevention measures.

Keywords: Phishing, social engineering, information security, cyberattack, psychological threats.

Bugungi kunda raqamli axborot vositalari jadal rivojlanar ekan, kiberxavfsizlik masalalari global muammoga aylanmoqda. Fishing va ijtimoiy muhandislik hujumlari, ayniqsa, foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlarini o‘g‘irlashda keng qo‘llanilmoqda [1].

Fishing va ijtimoiy muhandislik hujumlari – **bu** kiberjinoyatchilar tomonidan foydalanuvchilarni csalg‘itish orqali maxfiy ma’lumotlarni qo‘lga kiritish, tizimlarga kirish yoki zararli dasturlarni joylashtirish uchun amalga oshiriladigan hujumlar**.**

Bu turdagi hujumlarning maqsadi – login va parollarni o‘g‘irlash, bank kartalari va moliyaviy ma’lumotlarni qo‘lga kiritish, davlat tizimlariga noqonuniy kirish hamda tizimlarga zararli dasturlarni o‘rnatish.

1. Fishing hujumlari.

Fishing hujumi – bu firibgarlik usuli bo‘lib, hujumchilar soxta veb-saytlar, elektron pochta yoki xabarlar orqali foydalanuvchini aldab, undan maxfiy ma’lumotlarni olishga urinishdir**.**

Fishing hujumlarining asosiy xususiyatlari – hujum **f**oydalanuvchi haqiqiy deb hisoblaydigan manbadan bo‘ladi, hujumchi foydalanuvchini soxta veb-saytlarga yo‘naltirib, login va parollarni o‘g‘irlaydi hamda elektron pochta, SMS yoki ijtimoiy tarmoqlar orqali tarqatiladi.

Fishing hujumlarining asosiy turlari

1-jadval

Fishing turi	Tavsif
Email Phishing	Soxta elektron pochta orqali foydalanuvchini aldash
Spear Phishing	Maxsus bir shaxs yoki kompaniyaga qaratilgan fishing hujumi
Whaling	Yuqori lavozimli rahbarlarga qaratilgan fishing hujumi
Smishing	SMS orqali fishing xabarlari yuborish.
Vishing	Telefon qo‘ng‘iroqlari orqali fishing hujumi

Fishing hujumlarida hujumchi ishonchli tashkilot (masalan, bank, pochta, davlat idorasi) nomidan soxta xat yuboradi, ushbu xat orqali foydalanuvchidan ma’lumotlarini yangilash, parolni kiritish yoki havolaga bosish so‘raladi. Havola foydalanuvchini soxta saytga olib boradi, u esa asl saytdan deyarli farq qilmaydi. Foydalanuvchi ma’lumotlarini kiritgach, bu ma’lumotlar firibgarning qo‘liga tushadi.

F**ishing hujumlarining belgilari quyidagi bo‘lishi mumkin:**

tanish bo‘lmagan manzildan kelgan shubhali xabarlar;

“Hisobingiz bloklandi” kabi vahima uyg‘otuvchi matnlar;

“Tezda javob bering!” – vaqt bo‘yicha bosimlar;

Soxta manzil – https://paypa1.com (aslida esa paypal.com bo‘lishi kerak).

Fishing hujumlaridan himoyalanish uchun sayt manziliga e’tibor berish lozim (HTTPS bo‘lishi shart), emaildagi havolalarga darhol bosmaslik, parollarinni hech kimga aytmaslik, ikki bosqichli autentifikatsiyani yoqish hamda antifishing dasturlar va brauzer plaginlaridan foydalanish lozim bo‘ladi.

2. Ijtimoiy muhandislik hujumlari.

Ijtimoiy muhandislik hujumlarida texnik vositalardan ko‘ra, inson ishonchi va psixologiyasiga urg‘u beriladi. U quyidagi usullarni o‘z ichiga oladi [2]:

Ijtimoiy muhandislik **– bu** foydalanuvchilarning psixologik xususiyatlaridan foydalanib, ularni aldash va maxfiy ma’lumotlarni qo‘lga kiritish uchun ishlatiladigan hujum turi**.** Ijtimoiy muhandislik hujumlarining asosiy xususiyatlari shundaki, hujumchi foydalanuvchilarni maxfiy ma’lumotlarini qo‘lga kiritishni ishonchni

qozonish, manipulyatsiya qilish, hamda elektron pochta, qo‘ng‘iroqlar, shaxsiy uchrashuvlar yoki ijtimoiy tarmoqlar orqali amalga oshiradi.

Ijtimoiy muhandislik hujumlarni amalga oshirish uchun hujumchi tanlangan shaxs haqida ma’lumot to‘playdi (ismi, lavozimi, tashkilot, qiziqishlari) va unga ishonchli ko‘rinadigan muloqot yaratadi (masalan, tashkilot xavfsizlik bo‘limidanman deydi), hamda jabrlanuvchidan parol, login, yoki fayl yuborishni so‘raydi. Bunda jabrlanuvchi hech narsadan shubhalanmay harakat qiladi va hujum muvaffaqiyatli amalga oshadi [4].

Ijtimoiy muhandislik hujumlarining asosiy turlari

2-jadval

Hujum turi	Tavsif
Pretexting	O‘zini rasmiy shaxs sifatida ko‘rsatib, ma’lumot so‘rash
Baiting	Qiziqarli narsa (fleshka, sovg‘a, link) orqali foydalanuvchilarni zararli fayllarni yuklashga undash
Tailgating	Jismoniy xavfsizlikni buzib, ob’ektga ruxsatsiz kirish
Quid Pro Quo	Foydalanuvchiga soxta yordam (sovrinlar, lotereyalar) taklif qilish va ma’lumot olish

Misol: Telefon orqali bank xodimi sifatida qo‘ng‘iroq qilib, foydalanuvchidan parolni so‘raydi, **yoki** hujumchi kompaniya hisobchisi nomidan soxta xabar yuboradi: “Yangi yetkazib beruvchi uchun to‘lov qilish zarur. Quyidagi hisob raqamga pul o‘tkazing”. Shunda tashkilot hisobchisi xabarga ishonadi va mablag‘ni jinoyatchining hisobiga o‘tkazadi.

Ijtimoiy muhandislik hujumlaridan himoyalanish uchun shaxsiy ma’lumotlarni noma’lum shaxslarga bermaslik, qo‘ng‘iroqlar yoki elektron xabarlarda shubhali so‘rovlarni e’tiborsiz qoldirish, tizimga kirish huquqiga ega bo‘lgan xodimlarga xavfsizlik treninglari o‘tkazish hamda parollarni muntazam o‘zgartirish va xavfsiz saqlash lozim.

Real hayotdagi fishing va ijtimoiy muhandislik hujumlari [4]

3-jadval.

Yil	Hodisa	Jabrlangan tashkilot	O‘g‘irlangan ma’lumotlar
2020	Kredit karta ma’lumotlari o‘g‘irlandi	Target	40 million kredit karta ma’lumotlari o‘g‘irlangan

2022	Mashhur akkauntlar fishing qurboni bo‘ldi	Twitter	Bir nechta mashhur akkauntlar buzilgan
2023-2024	Muvaffaqiyatli fishing hujumi	Google & Facebook	$100 million yo‘qotgan

Tashkilotlarda ijtimoiy muhandislik hujumlaridan h**imoyalanish uchun h**ar qanday shubhali so‘rovga **javob bermaslik, x**odimlar bilan muntazam ravishda **kiberxavfsizlik bo‘yicha treninglar o‘tkazish**, har bir xodimning **vazifasiga doir doiraviy huquqlarni belgilash** va tashqi manba yoki shaxsdan kelgan har qanday talabni **tasdiqlash mexanizmini** ishlab chiqish tavsiya etiladi [5].

Ijtimoiy muhandislik hujumlaridan himoyalanish uchun kiberxavfsizlik bo‘yicha xodimlarni muntazam o‘qitish, ikki bosqichli autentifikatsiyadan va fishinglarni aniqlovchi tizimlardan foydalanish, hamda tashkilotning axborot xavfsizligi siyosatiga qat’iy rioya qilish kerak.

Xulosa qilib shuni aytish mumkinki, fishing va ijtimoiy muhandislik hujumlari – zamonaviy kiberxavfsizlik muammolarining markazida turadi. Bunday hujumlar texnologik emas, balki inson psixologiyasi orqali amalga oshiriladigan kiberxavflardir. Bunday tahdidlarga qarshi kurashda texnologik choralar bilan bir qatorda, foydalanuvchilarni o‘qitish va ogohlik darajasini oshirish zarur [6].

Foydalanilgan adabiyotlar ro‘yxati:

1. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.
2. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
3. Symantec. (2021). Internet Security Threat Report.
4. FBI. (2017). Lithuanian Man Charged with Theft of Over $100 Million. https://www.fbi.gov
5. ENISA. (2022). Cybersecurity Threat Landscape Report.
6. Alayev S.R. Axborot xavfsizligi asoslari. Darslik. Aloqa nashriyoti, Toshkent 2025 y.