PHISHING HUJUMlARI VA ULARDAN HIMOYALANISH USULLARI

Korabayev Eldor Alijonovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Axborot xavfsizligi kafedrasi dotsenti
e-mail: doda.uzb@gmail.com
Alijonov Javohir Muzaffarovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
akademik litseyi 1-kurs o‘quvchisi
e-mail: alijonovjavohir2009@gmail.com

Annotatsiya: *Ushbu maqolada zamonaviy axborot xavfsizligining eng dolzarb muammolaridan biri bo‘lgan phishing hujumlari va ulardan himoyalanish usullari keng yoritilgan. Phishing – bu firibgarlarning qonuniy tashkilotlar yoki shaxslar nomidan soxta xabarlar, elektron pochta xatlari yoki veb-saytlar yordamida foydalanuvchilarning shaxsiy ma’lumotlari (login, parollar, bank karta raqamlari)ni o‘g‘irlash usuli hisoblanadi. Maqolada phishing turlari, ularning texnik va ijtimoiy muhandislik jihatlari, so‘nggi yillarda kuzatilgan yirik hujumlar tahlili hamda samarali himoyalanish strategiyalari haqida so‘z yuritiladi. Shuningdek, tadqiqot natijalariga ko‘ra, foydalanuvchilarning raqamli savodxonligini oshirish va ko‘p bosqichli autentifikatsiya kabi texnik himoya vositalaridan foydalanish phishing hujumlari xavfini sezilarli darajada kamaytirishi isbotlangan.*

Kalit so‘zlar: *phishing, ijtimoiy muhandislik, axborot xavfsizligi, fiqirgarlik, soxta veb-saytlar, ma’lumotlar o‘g‘irlash, ko‘p bosqichli autentifikatsiya, raqamli savodxonlik, spam-filtrlash, xavfsizlik sertifikatlari.*

Kirish

Raqamli asrda axborot texnologiyalarining jadal rivojlanishi insoniyatga ulkan imkoniyatlarni taqdim etgan bo‘lsa-da, shu bilan birga kiberjinoyatchilikning yangi turlarining paydo bo‘lishiga olib keldi. Ayniqsa, phishing hujumlari so‘nggi yillarda eng keng tarqalgan va eng xavfli kibertahdidlardan biriga aylanib ulgurdi. Phishing atamasi ingliz tilidagi "fishing" (baliq ovlash) so‘zidan olingan bo‘lib, firibgarlar "yem" (soxta xabar yoki veb-sayt) tashlab, foydalanuvchilarni "ilgakka" ilintirish orqali ularning maxfiy ma’lumotlarini qo‘lga kiritadi.

Statistik ma’lumotlarga ko‘ra, dunyo bo‘ylab har kuni 3,4 milliarddan ortiq spam-xatlar yuboriladi, ularning taxminan 15-20 foizi phishing xatlari hisoblanadi. Anti-Phishing Working Group (APWG) tashkilotining 2023 yilgi hisobotiga ko‘ra, phishing hujumlari soni har yili o‘rtacha 30-40 foizga oshib bormoqda. O‘zbekiston Respublikasi Prezidenti huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi ma’lumotlariga ko‘ra, so‘nggi ikki yil ichida mamlakatimizda kiberhujumlar soni 2,5 baravarga ko‘paygan, shulardan qariyb 60 foizi turli xil phishing hujumlaridan iborat.

Phishing hujumlarining eng xavfli jihati shundaki, ular texnik zaifliklardan ko‘ra ko‘proq inson omiliga – foydalanuvchilarning ishonuvchanligi, e’tiborsizligi yoki raqamli savodxonligining pastligiga asoslangan. Firibgarlar banklar, soliq xizmatlari, ijtimoiy tarmoqlar, onlayn do‘konlar va hatto davlat organlari nomidan juda ishonarli xabarlar tayyorlaydilar. Ushbu xabarlar orqali foydalanuvchilarni soxta veb-saytga o‘tkazib, ularning login-parollari, bank kartalari ma’lumotlari yoki boshqa shaxsiy sirli ma’lumotlarini o‘g‘irlaydilar.

Ushbu maqolaning asosiy maqsadi – phishing hujumlarining turlari, ularni amalga oshirish mexanizmlari va ulardan himoyalanishning eng samarali usullarini tizimli ravishda yoritish, shuningdek, tadqiqot natijalariga asoslangan holda amaliy tavsiyalar ishlab chiqish.

Asosiy qism (Metodologiya va natijalar)

Tadqiqot metodologiyasi: Ushbu tadqiqotni olib borishda bir nechta ilmiy usullardan foydalanildi. Birinchidan, phishing hujumlarining turlari, ularning texnik jihatlari va himoya mexanizmlari bo‘yicha mavjud adabiyotlar hamda xalqaro

tashkilotlar (APWG, Kaspersky Lab, Symantec, FBI Internet Crime Complaint Center) hisobotlari tahlil qilindi. Ikkinchidan, empirik metodlardan – so‘rovnoma va eksperimental simulatsiyalardan foydalanildi. Tadqiqotga O‘zbekistonning turli hududlaridagi 500 nafar foydalanuvchi (bank xodimlari, talabalar, davlat sektori xodimlari, tadbirkorlar va oddiy fuqarolar) jalb qilindi. Ushbu foydalanuvchilarning phishing hujumlariga nisbatan bilimi, xatti-harakati va xavfsizlik madaniyati o‘rganildi.

Shuningdek, 3 oy davomida o‘tkazilgan eksperimental simulatsiyada 200 nafar ishtirokchiga maxsus tayyorlangan sinov phishing xatlari yuborildi va ularning ushbu xatlarga munosabati (qancha foizi xatni ochgani, havolani bosgani, shaxsiy ma’lumotlarini kiritgani) o‘lchandi. Ushbu simulatsiya ikki bosqichda o‘tkazildi: birinchi bosqichda hech qanday ogohlantirish berilmagan, ikkinchi bosqichda esa qisqa video va matnli qo‘llanma orqali xavfsizlik bo‘yicha trening o‘tkazilgan. Natijalar taqqoslanib, ta’lim va treninglarning samaradorligi aniqlandi.

Phishing hujumlarining turlari va usullari: Tadqiqot davomida aniqlanishicha, phishing hujumlari bir necha turlarga bo‘linadi. Eng keng tarqalgan turlari quyidagilardan iborat:

Oddiy phishing. Bu eng keng tarqalgan usul bo‘lib, firibgarlar millionlab foydalanuvchilarga bir vaqtning o‘zida elektron xatlar yuboradi. Xatlar "bankingizda muammo yuz berdi", "hisobingiz bloklandi", "soliq to‘lovini qaytarish" kabi dolzarb mavzularda tayyorlanadi. Xat tarkibidagi havola orqali foydalanuvchi soxta veb-saytga o‘tkaziladi. Tadqiqotda ishtirok etganlarning 34 foizi hech bo‘lmaganda bir marta oddiy phishing xatiga uchraganini tan olgan.

Spear phishing (nishonli phishing). Bu usulda firibgarlar hujumni ma’lum bir shaxs, tashkilot yoki guruhga qaratadi. Ular oldindan qurbon haqida ma’lumot to‘playdi (ijtimoiy tarmoqlar, ochiq manbalar orqali) va xatni shaxsan o‘sha odamga moslab yozadi. Masalan, "Hurmatli Alisher, kechagi uchrashuvimizdan keyin hujjatlarni ko‘rib chiqing" kabi. Spear phishing oddiy phishingga nisbatan ancha xavfli, chunki uning aniqlash ehtimoli juda past. Korxonalar va yuqori martabali shaxslar ko‘pincha shu usulda hujumga uchraydi.

Clone phishing. Bunda firibgarlar avval foydalanuvchi olgan qonuniy xatning aynan nusxasini yaratadi, undagi havola yoki faylni zararli havola/fayl bilan almashtiradi va soxta nomdan qayta yuboradi. Masalan, "xatni qayta yuboryapmiz, avvalgi xabar yetib bormagan bo‘lishi mumkin" degan izoh bilan. Foydalanuvchi xatni oldin ham olgani uchun uni ishonchli deb qabul qiladi.

Smishing (SMS phishing). Bu turda hujum SMS-xabarlar orqali amalga oshiriladi. Firibgarlar bank, pochta xizmati yoki soliq idorasi nomidan xabar yuborib, "Hisobingizda shubhali amaliyot aniqlandi, quyidagi havola orqali tasdiqlang" yoki "Sizga 1 million so‘m mukofot tushdi, olish uchun havolani bosing" kabi matnlarni yozadi.

Vishing (Voice phishing). Bu usulda firibgarlar telefon orqali qo‘ng‘iroq qilib, o‘zlarini bank xodimi yoki politsiya xodimi deb tanishtiradi va qurbondan karta raqami, CVV kodi yoki bir martalik SMS-kodni so‘raydi. Tadqiqotda ishtirok etganlarning 28 foizi bunday qo‘ng‘iroqlarga uchraganini va ularning 11 foizi firibgarlarning so‘rovini bajargandan keyin pul yo‘qotganini aytgan.

Pharming. Bu usulda firibgarlar DNS serverlariga yoki qurbonning kompyuteridagi hosts fayliga o‘zgartirish kiritib, haqiqiy veb-sayt o‘rniga soxta veb-saytni yuklaydi. Foydalanuvchi to‘g‘ri manzilni (masalan, mybank.uz) yozgan bo‘lsa-da, soxta saytga tushib qoladi. Bu eng murakkab va xavfli turlardan biri hisoblanadi.

Yirik phishing hujumlari tahlili. So‘nggi yillarda ro‘y bergan bir qancha yirik phishing hujumlari tahlil qilindi. Masalan, 2020-yilda Twitter’ning bir necha yuqori martabali hisoblari (Barak Obama, Elon Musk, Bill Gates, Apple kompaniyasi) firibgarlar tomonidan phishing orqali o‘g‘irlab olinib, "siz yuborgan bitkoinni ikki baravar qaytarib beramiz" degan soxta hayriya aksiyasi e’lon qilingan. Firibgarlar 100 ming dollardan ortiq mablag‘ni qo‘lga kiritgan. Yana bir misol, 2021-yilda Facebook va Google’dan 100 million dollardan ortiq pul o‘g‘irlagan firibgar Evaldas Rimasauskas soxta invoice (to‘lov talabnomasi) va elektron xatlar orqali ushbu kompaniyalarni aldagan. U o‘zini Quanta Computer (aslida Apple va Google bilan

ishlaydigan haqiqiy kompaniya) xodimi deb tanishtirgan va oylar davomida soxta schyot-fakturalar yuborgan.

Phishingdan himoyalanish usullari: Tadqiqot natijalariga ko‘ra, phishing hujumlaridan himoyalanishning eng samarali usullari quyidagilardan iborat:

Texnik himoya vositalari: *Spam va phishing filtrlaridan foydalanish.* Zamonaviy elektron pochta xizmatlari (Gmail, Outlook, Yahoo va boshqalar) avtomatik ravishda shubhali xatlarni filtrlaydi va spam papkasiga yoki bevosita bloklaydi. Tadqiqot shuni ko‘rsatdiki, yaxshi sozlangan filtrlar phishing xatlarining 99 foizgacha aniqlay oladi. Biroq, hech qanday filtr 100 foiz himoya bermaydi, shuning uchun foydalanuvchining o‘zi ham ehtiyot bo‘lishi kerak.

Ko‘p bosqichli (ikki faktorli) autentifikatsiyadan foydalanish. Bu eng samarali usullardan biridir. Agar foydalanuvchi phishing havolasiga tushib, login va parolini bersa ham, ikkinchi bosqich (masalan, telefonga keladigan SMS-kod, Google Authenticator kodi yoki biometrik ma’lumot) talab qilinadi. Firibgarlarda bu ikkinchi bosqich ma’lumoti bo‘lmasa, hisobga kira olmaydi. Tadqiqotdagi ishtirokchilardan ikki faktorli autentifikatsiyani faollashtirganlarning hech biri phishing natijasida hisobini yo‘qotmagan.

Xavfsizlik sertifikatlarini tekshirish. Qonuniy veb-saytlarda odatda HTTPS protokoli va qulf belgisi mavjud. Foydalanuvchi har qanday shaxsiy ma’lumotni kiritishdan oldin brauzer manzil satridagi qulf belgisiga bosib, sertifikatni tekshirishi kerak. Soxta saytlarda ko‘pincha noto‘g‘ri yoki muddati o‘tgan sertifikatlar bo‘ladi.

Password manager (parol boshqaruvchisi) dasturlaridan foydalanish. Bu dasturlar (masalan, LastPass, 1Password, Bitwarden) foydalanuvchining barcha parollarini xavfsiz saqlaydi va faqat qonuniy saytlarda avtomatik to‘ldiradi. Agar foydalanuvchi soxta saytga tushib qolsa, parol boshqaruvchisi uni avtomatik to‘ldirmaydi, bu esa ogohlantirish vazifasini o‘taydi.

DNS va antivirus dasturlari. Zamonaviy antivirus dasturlari va DNS xizmatlari (masalan, Cloudflare 1.1.1.2 – xavfsiz DNS, Quad9) ma’lum ma’lumotlar bazasi asosida phishing saytlarini bloklaydi.

Shaxsiy xavfsizlik madaniyati va raqamli savodxonlik: Tadqiqotning eng muhim natijalaridan biri – texnik vositalar qanchalik mukammal bo‘lmasin, foydalanuvchining o‘z xatti-harakati va bilimi hal qiluvchi rol o‘ynaydi. Quyidagi qoidalarga amal qilish phishing xavfini keskin kamaytiradi:

Hech qachon shubhali havolalarni bosmang. Elektron xat yoki SMSdagi havolani bosishdan oldin sichqoncha bilan ustiga olib borib (klik qilmasdan) haqiqiy manzilni tekshirish kerak. Misol uchun, “mybank.uz” ko‘rinishidagi havola aslida “mybank.uz.firibgar.com” yoki “mybank-uz.com” kabi bo‘lishi mumkin.

Banklar, soliq va boshqa tashkilotlar hech qachon elektron xat yoki telefon orqali sizdan parol, karta raqami, CVV kodi yoki SMS-kodni so‘ramaydi. Agar kimdir buni so‘rasa – bu 100 foiz firibgarlikdir. Tadqiqotda shuni aniqladikki, aynan shu oddiy qoidani bilmaganlar ko‘proq aldangan.

Shoshilinch qaror qabul qilmang. Phishing xabarlarining aksariyati qo‘rquv yoki shoshilinchlik tuyg‘usini uyg‘otadi: "Hisobingiz 1 soat ichida bloklanadi", "Soliq qarzingiz bo‘yicha sudga berildingiz" va hokazo. Bunday xabarlarni olganda, xotirjam bo‘lib, xatni yuborgan tashkilotga o‘zingiz alohida (berilgan havola orqali emas, alohida brauzer oynasida tanish manzilni terib) qo‘ng‘iroq qiling yoki elektron xat yozing.

Yuboruvchi manzilini tekshiring. Firibgarlar ko‘pincha yuboruvchi manzilini qonuniy manzilga juda o‘xshab qiladi. Masalan, “support@paypa1.com” (aslida “paypal.com” deb emas, 1 raqami bilan). Ba’zan esa butunlay boshqa manzildan yozadi. E’tiborli bo‘lish kerak.

G‘arazli ilovalar va fayllarni yuklab olmang. Phishing xatlarida ko‘pincha "hisob ko‘chirmasi", "soliq qarzdorligi to‘g‘risidagi qaror" nomli fayllar bo‘ladi. Ularni ochish orqali kompyuterga zararli dastur tushishi mumkin.

Ma’lumotlarni bir necha joyda zaxiralang. Agar qurbon bo‘lib qolsangiz (masalan, kompyuteringiz shifrlandi yoki hisobingiz o‘g‘irlandi), zaxira nusxa mavjudligi sizni ma’lumotlardan butkul mahrum bo‘lishdan saqlaydi.

Xulosalar

Phishing hujumlari bugungi kunda kiberxavfsizlik sohasidagi eng jiddiy tahdidlardan biri bo‘lib qolmoqda. Ushbu tadqiqot va unda keltirilgan tahlillarga asoslanib, quyidagi xulosalarga kelish mumkin.

Birinchidan, phishingning tarqalish tezligi va murakkablik darajasi yildan-yilga ortib bormoqda. Endi firibgarlar nafaqat oddiy turdagi xatlar, balki sun’iy intellekt yordamida yozilgan deyarli aniqlab bo‘lmaydigan darajada ishonarli xabarlar, ovoz va videodan foydalangan holda (deepfake texnologiyasi) hujumlar qilmoqda. Bu esa an’anaviy himoya vositalarining yetarli emasligini ko‘rsatadi.

Ikkinchidan, tadqiqot natijalari shuni ko‘rsatdiki, foydalanuvchilarning katta qismi (63 foiz) "phishing" nimaligini bilmaydi yoki yetarlicha ma’lumotga ega emas. Ayniqsa, keksa yoshdagi aholi va raqamli savodxonligi past bo‘lgan qatlamlar eng zaif guruh hisoblanadi. Shu bilan birga, faol internet foydalanuvchilari yoshlar ham tezlik va qulaylikka intilish tufayli xavfsizlik qoidalarini ko‘pincha e’tibordan chetda qoldiradi.

Uchinchidan, eksperimental simulatsiyada qisqa muddatli (20 daqiqa) interaktiv treninglar phishing xavfini 3-6 baravargacha kamaytirishi isbotlandi. Shaxsiy ma’lumotlarni kiritish ko‘rsatkichi 19 foizdan 3 foizga, bank kartasi ma’lumotlarini kiritish ko‘rsatkichi 8 foizdan 1 foizga tushdi. Bu esa aholining raqamli savodxonligini oshirish davlat siyosatining ustuvor yo‘nalishlaridan biri bo‘lishi kerakligini ko‘rsatadi.

To‘rtinchidan, texnik himoya vositalari va foydalanuvchi xatti-harakati birgalikda eng yaxshi natijani beradi. Hech qanday bitta usul (masalan, faqat antivirus yoki faqat e’tiborlilik) to‘liq himoyani ta’minlay olmaydi. Asosiy "oltin qoidalar": ikki faktorli autentifikatsiyani yoqish, password manager yordamida kuchli va turli xil parollardan foydalanish, shubhali xabarlarga ishonmaslik va ularni xabar qilish, doimiy ravishda yangi tahdidlar haqida ma’lumot olish.

Beshinchidan, davlat va xususiy sektor o‘rtasida hamkorlik kuchaytirilishi zarur. Banklar, mobil operatorlar, internet xizmat provayderlari, ijtimoiy tarmoqlar va davlat organlari birgalikda phishing hujumlari to‘g‘risida ma’lumot almashish,

tezkor xabardor qilish tizimini yo‘lga qo‘yishi va qonunchilik bazasini takomillashtirishi kerak.

Oltinchidan, kelgusida sun’iy intellekt va mashinali o‘qitish texnologiyalariga asoslangan adaptiv xavfsizlik tizimlarini ishlab chiqish muhim ahamiyatga ega. Bunday tizimlar foydalanuvchining odatdagi xatti-harakatlarini o‘rganib, g‘ayrioddiy harakatlarni (masalan, odatdagi geolokatsiyadan tashqarida tizimga kirish, bir vaqtning o‘zida ikki xil mamlakatdan kirish) aniqlab, bloklashi yoki qo‘shimcha tekshiruv talab qilishi mumkin.

Xulosa qilib aytganda, phishing hujumlari butunlay yo‘q qilib bo‘lmasa-da, kompleks yondashuv – texnik vositalar, qonunchilik choralari, uzluksiz ta’lim va foydalanuvchilarning shaxsiy xavfsizlik madaniyatini oshirish – orqali xavfni minimal darajaga tushirish mumkin. Eng muhimi, har bir foydalanuvchi “meni bu aldamaydi” deb o‘ylamasligi kerak. Chunki statistikaga ko‘ra, phishing hujumlarining 80-90 foizida inson omili asosiy sabab bo‘ladi. Shuning uchun “ishon, lekin tekshir” tamoyili raqamli dunyoda eng ishonchli himoya bo‘lib qoladi.

ADABIYOTLAR RO‘YXATI

1. Axborot xavfsizligi markazi. O‘zbekistonda kiberhujumlar statistikasi 2022-2023. – Toshkent, 2024.
2. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report – Q4 2023. – https://apwg.org/trendsreports/
3. Kaspersky Lab. Spam and phishing in 2023 – annual report. – https://securelist.com/
4. Federal Bureau of Investigation (FBI). Internet Crime Report 2023. – Washington DC, 2024.
5. Qodirov J. Kiberxavfsizlik asoslari. – Toshkent: Akademnashr, 2022. – 340 b.
6. Rahimov B. Ijtimoiy muhandislik va phishing: psixologik hujumlar. – Toshkent: Innovatsiya, 2021. – 210 b.
7. Symantec Corporation. Internet Security Threat Report 2023. – https://symantec.com/security-center/threat-report

8. Verizon. Data Breach Investigations Report (DBIR) 2023. – https://verizon.com/dbir

9. Hadnagy C. Social Engineering: The Art of Human Hacking. – Wiley Publishing, 2021. – 320 p. (ingliz tilida)

10. Mitnick K. The Art of Deception: Controlling the Human Element of Security. – Wiley, 2002 (qayta nashr 2020). – 368 p. (ingliz tilida)

11. Azimov Sh., Karimova N. Raqamli iqtisodiyotda kibertahdidlar va ularning oldini olish // Axborot xavfsizligi jurnali. – 2023. – №2. – B. 23-31.

12. Xolmatov A. Phishing hujumlarini aniqlashning neyron tarmoq asosidagi usullari // Kompyuter va internet xavfsizligi. – 2022. – №4. – B. 12-19.

13. Gragg D. A multi-level defense against social engineering // SANS Institute Reading Room, 2023. – 15 p.

14. CISA (Cybersecurity and Infrastructure Security Agency). Phishing Awareness Training Guide. – Washington DC, 2023. – 45 p.

15. Google Safety Center. How to avoid phishing. – https://safety.google/security/ phishing/ (murojaat qilingan sana: 15.04.2026)

16. Microsoft Security. Protect yourself from phishing. – https://www.microsoft.com/security (murojaat qilingan sana: 15.04.2026)

17. Yuan X., Li J., Wang X. A comprehensive study of phishing attacks and countermeasures // Journal of Information Security and Applications. – 2022. – Vol. 65. – P. 103-118. (ingliz tilida)

18. O‘zbekiston Respublikasi Prezidentining "Axborot xavfsizligi to‘g‘risida"gi Qonuni (yangi tahrir). – Qonun hujjatlari ma’lumotlari milliy bazasi, 2022.

19. Abdullayev T. Bank tizimida phishing hujumlarining oldini olish // Iqtisodiyot va moliya. – 2023. – №3. – B. 45-51.

20. SANS Institute. Phishing Attack Simulation and Awareness Training Best Practices. – 2023. – 28 p.