"JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN" JURNALI
VOLUME 04, ISSUE 06, 2026. JUNE
ResearchBib Impact Factor: 9.654/2024 ISSN 2992-8869

PHISHING HUJUMLARINI ANIQLASH VA OLDINI OLISHNING ZAMONAVIY YONDASHUVLARI

Mamatova Husnida Xatamjon qizi
Farg'ona davlat texnika universiteti katta o'qituvchisi, (PhD)
E-mail: *hmx2605@gmail.com*
Karimjonov Shahzodbek Jahongir o'g'li
Farg'ona davlat texnika universiteti, 2-bosqich talabasi
E-mail: *shahzodbekkarimjonov195@gmail.com*

Annotatsiya. *Mazkur maqolada phishing hujumlarining kelib chiqish sabablari, asosiy ko'rinishlari, aniqlash mezonlari hamda ularning oldini olish usullari kiberxavfsizlik nuqtayi nazaridan tahlil qilinadi. Phishing foydalanuvchilarni aldash orqali login va parollar, bank karta ma'lumotlari, elektron pochta akkauntlari, ta'lim platformalaridagi hisoblar hamda tashkilotlarga oid maxfiy axborotlarni qo'lga kiritishga qaratilgan ijtimoiy muhandislik hujumlarining keng tarqalgan turi hisoblanadi. Bunday hujumlar elektron pochta, SMS xabarlari, messenjerlar, telefon qo'ng'iroqlari, QR-kodlar va soxta veb-sahifalar orqali amalga oshiriladi.*

Maqolada ta'lim muassasalarida phishing xavfini kamaytirish, raqamli savodxonlikni oshirish va kiberxavfsizlik madaniyatini shakllantirishga qaratilgan amaliy tavsiyalar keltirilgan. Shuningdek, ko'p faktorli autentifikatsiya, xavfsiz parol siyosati, elektron pochta gigiyenasi va kiberxavfsizlik hodisalariga tezkor javob berish mexanizmlarining ahamiyati yoritilgan. Tadqiqot natijalari ta'lim muassasalari xodimlari, professor-o'qituvchilar, talabalar hamda internetdan foydalanuvchi keng jamoatchilik uchun foydali bo'lishi mumkin.

Kalit so'zlar: *phishing, kiberxavfsizlik, ijtimoiy muhandislik, spear phishing, smishing, vishing, quishing, spoofing, zararli havola, autentifikatsiya, MFA, passkey, elektron pochta xavfsizligi, raqamli savodxonlik, ta'lim muassasasi.*

MODERN APPROACHES TO DETECTING AND PREVENTING PHISHING ATTACKS

Mamatova Husnida Xatamjon qizi
Fergana state technical university Senior Lecturer, PhD
E-mail: *hmx2605@gmail.com*
Karimjonov Shahzodbek Jahongir o'g'li
Second-Year Student, Cybersecurity Program, Fergana State Technical University
E-mail: *shahzodbekkarimjonov195@gmail.com*

Abstract. *This article analyzes the causes, main forms, detection criteria, and prevention methods of phishing attacks from a cybersecurity perspective. Phishing is one of the most common types of social engineering attacks aimed at obtaining users' confidential information, including usernames and passwords, bank card details, email accounts, educational platform accounts, and organization-related sensitive data by deceiving users. Such attacks are commonly carried out through email messages, SMS messages, instant messengers, phone calls, QR codes, and fraudulent websites.*

The article provides practical recommendations for reducing phishing risks in educational institutions, improving digital literacy, and promoting a cybersecurity culture. It also highlights the importance of multi-factor authentication, strong password policies, email security hygiene, and rapid incident response mechanisms. The findings of the study may be beneficial for employees of educational institutions, academic staff, students, and the broader community of Internet users.

Keywords*: phishing, cybersecurity, social engineering, digital literacy, multi-factor authentication, email security, information security, educational institutions.*

СОВРЕМЕННЫЕ ПОДХОДЫ К ВЫЯВЛЕНИЮ И ПРЕДОТВРАЩЕНИЮ ФИШИНГОВЫХ АТАК

Маматова Хуснида Хатамжон кизи
Ферганский государственный технический университет старший преподаватель, PhD
E-mail: *hmx2605@gmail.com*
Каримжонов Шаҳзодбек Жаҳонгир ўғли
Студент 2 курса Ферганский государственный технический университет
E-mail: *shahzodbekkarimjonov195@gmail.com*

Аннотация. *В данной статье с точки зрения кибербезопасности анализируются причины возникновения фишинговых атак, их основные виды, критерии выявления и методы предотвращения. Фишинг является одним из наиболее распространённых видов атак социальной инженерии, направленных на получение конфиденциальной информации пользователей, такой как логины и пароли, данные банковских карт, учётные записи электронной почты, аккаунты образовательных платформ и сведения, относящиеся к деятельности организаций, путём введения пользователей в заблуждение. Подобные атаки обычно осуществляются через электронную почту, SMS-сообщения, мессенджеры, телефонные звонки, QR-коды и поддельные веб-страницы.*

В статье представлены практические рекомендации, направленные на снижение риска фишинговых атак в образовательных учреждениях, повышение цифровой грамотности и формирование культуры кибербезопасности. Кроме того, рассматривается значение многофакторной аутентификации, политики надёжных паролей, гигиены электронной почты и механизмов оперативного реагирования на инциденты кибербезопасности. Результаты исследования могут быть полезны сотрудникам образовательных учреждений, профессорско-преподавательскому составу, студентам, а также широкому кругу пользователей сети Интернет.

Ключевые слова: *фишинг, кибербезопасность, социальная инженерия, цифровая грамотность, многофакторная аутентификация, безопасность электронной почты, информационная безопасность, образовательные учреждения.*

Kirish

Raqamli texnologiyalar ta’lim jarayonining ajralmas qismiga aylandi. Elektron jurnal, masofaviy ta’lim platformalari, bulutli xotira, onlayn test tizimlari, ijtimoiy tarmoqlar va elektron pochta o‘qituvchi hamda talabalarning kundalik faoliyatida keng qo‘llanmoqda. Ushbu imkoniyatlar bilim olish va axborot almashinuvini tezlashtiradi, biroq shu bilan birga kiberxavfsizlik tahdidlarini ham kuchaytiradi. Eng ko‘p uchraydigan tahdidlardan biri phishing hisoblanadi. Phishing hujumi faqat texnik zaiflikdan emas, balki inson omilidan ham foydalanadi. Hujumchi

foydalanuvchining ishonchi, shoshqaloqligi, qo‘rquvi, qiziqishi yoki e’tiborsizligidan foydalanib, uni zararli havolaga kirishga, soxta sahifaga ma’lumot kiritishga yoki xavfli faylni ochishga majbur qiladi. Shuning uchun phishingga qarshi himoya nafaqat antivirus va xavfsizlik devori bilan, balki bilim, hushyorlik va to‘g‘ri odatlar bilan ham bog‘liq. Anti-Phishing Working Group ma’lumotlariga ko‘ra, 2025-yil davomida phishing hujumlari yuqori darajada saqlanib qoldi; 2025-yilning to‘rtinchi choragida 853 244 ta phishing hujumi qayd etilgan. Bu raqamlar phishingning global miqyosdagi dolzarbligini ko‘rsatadi. Ta’lim muassasalari ham bunday hujumlardan mustasno emas, chunki ularda shaxsiy ma’lumotlar, baholash natijalari, ilmiy ishlanmalar, moliyaviy hujjatlar va ko‘plab akkauntlar mavjud. Maqolaning maqsadi phishing hujumlarini ilmiy va amaliy jihatdan yoritish, o‘qituvchi hamda talabalar uchun aniq tavsiyalar ishlab chiqish va ta’lim muhitida xavfsiz raqamli madaniyatni shakllantirishga yordam berishdan iborat.

Phishing tushunchasi va uning kiberxavfsizlikdagi o‘rni

Phishing ingliz tilidagi “fishing” so‘ziga o‘xshash bo‘lib, mazmunan foydalanuvchini “qarmoqqa ilintirish”ni anglatadi. Kiberjinoyatchi o‘zini bank, universitet, davlat idorasi, texnik yordam xizmati, ijtimoiy tarmoq yoki tanish shaxs sifatida ko‘rsatadi. Maqsad foydalanuvchidan maxfiy ma’lumot olish yoki uni zararli amal bajarishga undashdir. Phishing ko‘pincha ijtimoiy muhandislikning bir shakli sifatida qaraladi. Ijtimoiy muhandislikda inson xatti-harakati, psixologik ta’sir va ishonch omillari asosiy rol o‘ynaydi. Masalan, xabarda “akkauntingiz bloklanadi”, “stipendiya to‘lovi uchun ma’lumotlaringizni tasdiqlang”, “dekanatdan muhim xabar” yoki “parolingiz muddati tugadi” kabi jumlalar bo‘lishi mumkin. Bunday iboralar foydalanuvchini tez qaror qabul qilishga undaydi. Phishingning asosiy xavfi shundaki, u oddiy foydalanuvchini murakkab texnik bilimlarsiz ham nishonga oladi. Agar foydalanuvchi o‘z parolini soxta saytga kiritib qo‘ysa, eng kuchli texnik himoya ham kechikkan bo‘lishi mumkin. Shu sababli phishingga qarshi kurashda inson omili markaziy ahamiyatga ega.

Phishing hujumlarining asosiy turlarini ko‘rib chiqish muhim. Phishing bir xil shaklda kechmaydi. Hujumchilar vaziyat, auditoriya va maqsadga qarab turli usullardan foydalanadilar. Quyida ta’lim muhitida ham uchrashi mumkin bo‘lgan asosiy ko‘rinishlar bayon qilinadi.

Elektron pochta phishingi. Bu eng keng tarqalgan turdir. Foydalanuvchiga rasmiy tashkilot nomidan soxta xat yuboriladi. Xatda “hisobingizni tasdiqlang”,

“ilovani yuklab oling”, “parolingizni yangilang” kabi chaqiriqlar mavjud bo‘ladi. Havola bosilganda foydalanuvchi haqiqiy saytga o‘xshash soxta sahifaga o‘tadi.

Spear phishing aniq bir shaxs yoki guruhga moslashtirilgan hujumdir. Masalan, hujumchi o‘qituvchining ismi, fani, kafedrasi yoki guruh nomidan foydalanib xabar yuboradi. Bunday xabar oddiy phishingga qaraganda ishonchliroq ko‘rinadi.

Whaling yuqori lavozimli shaxslar, masalan, rektor, dekan, kafedra mudiri, buxgalteriya xodimi yoki tizim administratoriga qaratiladi. Maqsad odatda yirik moliyaviy zarar yetkazish, ichki tizimga kirish yoki muhim hujjatlarni qo‘lga kiritishdir.

Smishing SMS yoki messenjerlar orqali, vishing esa telefon qo‘ng‘iroqlari orqali amalga oshiriladi. Hujumchi o‘zini bank, universitet yoki texnik yordam xodimi sifatida tanishtirib, parol, SMS-kod, karta raqami yoki boshqa maxfiy ma’lumotlarni so‘rashi mumkin.

QR phishing yoki quishing foydalanuvchini QR-kod orqali zararli manzilga yo‘naltiradi. Ta’lim muassasalarida QR-kodlar davomat, so‘rovnoma yoki ro‘yxatdan o‘tishda ishlatilgani uchun bu usul ayniqsa ehtiyotkorlikni talab qiladi.

Clone phishingda avvalgi haqiqiy xatga o‘xshash xabar yuborilib, uning ichidagi havola yoki fayl zararli variantga almashtiriladi. Business Email Compromise esa rahbar yoki hamkasb nomidan pul o‘tkazish, ma’lumot yuborish yoki muhim amal bajarishni talab qiluvchi firibgarlik turidir.

1-jadval. Phishing hujumlari turlarining tarqalish darajasi, xavflilik ko‘rsatkichi

Phishing turi	**Tarqalish darajasi**	**Xavflilik darajasi**	**Asosiy nishon**
Elektron pochta phishingi	Yuqori	O‘rta	Barcha foydalanuvchilar
Spear phishing	O‘rta	Yuqori	Muayyan shaxs yoki guruh
Whaling	Past	Juda yuqori	Rahbarlar va menejerlar
Smishing	Yuqori	O‘rta	Mobil foydalanuvchilar
Vishing	O‘rta	O‘rta	Telefon foydalanuvchilari

QR phishing (Quishing)	O‘sib bormoqda	Yuqori	QR-koddan foydalanuvchilar

Jadvaldan ko‘rinib turibdiki, elektron pochta phishingi eng keng tarqalgan hujum turi hisoblanadi. Biroq whaling va spear phishing hujumlari kamroq uchrasada, ular tashkilotlar uchun katta moliyaviy va axborot xavfini yuzaga keltiradi. So‘nggi yillarda QR-kodlardan foydalanish ortgani sababli quishing hujumlari ham sezilarli darajada ko‘paymoqda.

Phishingning psixologik mexanizmlari

Phishingning muvaffaqiyati ko‘pincha texnik murakkablikdan ko‘ra psixologik ta’sir kuchiga bog‘liq. Hujumchi foydalanuvchini fikrlashga emas, tez va hissiy qaror qabul qilishga undaydi. Shuning uchun phishing xabarlarida shoshilinchlik, qo‘rquv, mukofot va’da qilish, obro‘li tashkilot nomidan foydalanish kabi usullar ko‘p uchraydi. Shoshilinchlik hissi hujumchining eng asosiy qurolidir. “24 soat ichida tasdiqlang”, “aks holda akkauntingiz yopiladi” yoki “hoziroq javob bering” kabi iboralar foydalanuvchining tanqidiy fikrlashini pasaytiradi. Qo‘rquv uyg‘otuvchi xabarlar ham shunga o‘xshash ishlaydi: foydalanuvchi zarar ko‘rmaslik uchun havolani bosishga moyil bo‘ladi. Mukofot va’da qilish ham keng tarqalgan usuldir. “Grant yutdingiz”, “bepul kursga qabul qilindingiz”, “stipendiya uchun ro‘yxatdan o‘ting” kabi takliflar ayniqsa talabalar orasida qiziqish uyg‘otadi. Biroq haqiqiy tashkilotlar odatda maxfiy ma’lumotlarni norasmiy havola orqali so‘ramaydi. Ishonch omilidan foydalanish ta’lim muhitida xavfliroq bo‘lishi mumkin. Agar xabar o‘qituvchi, dekanat yoki universitet nomidan kelsa, talaba uni tezroq qabul qiladi. Agar o‘qituvchining akkaunti buzilgan bo‘lsa, uning nomidan yuborilgan xabarlar ko‘plab talabalar uchun ishonchli tuyulishi mumkin.

Phishing xabarlarini aniqlash belgilari

Phishingni aniqlash uchun foydalanuvchi xabarni mazmuni, yuboruvchi manzili, havola, ilova va kontekst bo‘yicha tekshirishi kerak. CISA phishing xabarlarida zararli havolalar, shubhali ilovalar, shaxsiy ma’lumot so‘rovlari va ishonchli manbaga o‘xshatish holatlariga alohida e’tibor berishni tavsiya qiladi.

Yuboruvchi manzilida kichik farqlar bo‘lishi: masalan, rasmiy domen nomi o‘rniga unga o‘xshash, lekin noto‘g‘ri yozilgan domen ishlatilishi.

Havola matni rasmiy ko‘rinsa ham, uning haqiqiy manzili boshqa saytga olib borishi.

Xabarda parol, SMS-kod, PIN-kod, karta raqami yoki pasport ma’lumotlari so‘ralishi.

“Darhol bosing”, “tezda tasdiqlang”, “akkauntingiz bloklanadi” kabi shoshilinch bosim beruvchi iboralar ishlatilishi.

Kutilmagan fayl ilovalari, ayniqsa .exe, .zip, .rar, .js, .scr yoki makrosli Office hujjatlari yuborilishi.

Rasmiy uslubga mos kelmaydigan imlo, tarjima, logo yoki dizayn xatolari mavjudligi.

Xabar kontekstining g‘alatiligi: siz kutmagan hujjat, topshiriq, to‘lov yoki so‘rov kelishi.

Biroq zamonaviy phishing xabarlari sun’iy intellekt yordamida juda ravon va rasmiy uslubda yozilishi mumkin. Shuning uchun faqat imlo xatolariga tayanish yetarli emas. Har bir foydalanuvchi havola, domen, so‘rov mazmuni va xabar kelgan vaziyatni kompleks baholashi zarur.

Ta’lim muassasalarida phishing xavfi

Ta’lim muassasalari, davlat tashkilotlari, xususiy korxonalar va oddiy internet foydalanuvchilari phishing hujumlari uchun jozibador nishon hisoblanadi. Chunki ushbu subyektlarning barchasi muhim ma’lumotlar va raqamli hisob qaydnomalardan foydalanadi. Buning sababi ularda ko‘p sonli foydalanuvchilar, turli axborot tizimlari, shaxsiy ma’lumotlar, ilmiy ishlanmalar, moliyaviy hujjatlar va baholash natijalari mavjudligidir. Universitet yoki maktabdagi bitta zaif akkaunt butun tizim xavfsizligiga ta’sir ko‘rsatishi mumkin. O‘qituvchilar ko‘p sonli elektron xat, talabalar ishlari, baholash fayllari, rasmiy hujjatlar va havolalar bilan ishlaydi. Bu esa zararli faylni tasodifan ochish yoki soxta havolaga kirish ehtimolini oshiradi. Talabalar esa ijtimoiy tarmoqlar, onlayn kurslar, grant e’lonlari va turli ro‘yxatdan o‘tish sahifalaridan faol foydalangani uchun phishingga duch kelishi mumkin. Agar o‘qituvchi akkaunti buzilsa, hujumchi uning nomidan talabalarga xabar yuborishi mumkin. Agar talaba akkaunti buzilsa, uning shaxsiy ma’lumotlari, baholari, elektron pochtasi yoki boshqa xizmatlari xavf ostida qoladi. Shu sababli kiberxavfsizlik masalasi faqat IT bo‘limining emas, balki butun ta’lim hamjamiyatining umumiy vazifasidir.

Phishingni oldini olishning asosiy usullari

Phishingga qarshi kurash kompleks yondashuvni talab qiladi. Texnik himoya, foydalanuvchi savodxonligi, aniq siyosat va tezkor xabar berish tizimi birgalikda

ishlaganda samaradorlik ortadi. Quyidagi usullar o‘qituvchi va talabalar uchun amaliy ahamiyatga ega. Birinchi navbatda raqamli savodxonlikni oshirish zarur. Har semestrda qisqa treninglar, amaliy mashg‘ulotlar, real phishing namunalarini tahlil qilish va xavfsizlik eslatmalarini tarqatish foydali bo‘ladi. NIST tashkilotlarga foydalanuvchilar phishingni taniy olishi, muntazam o‘qitilishi va phishingga tushib qolganini qanday xabar qilishni bilishi kerakligini tavsiya qiladi. Ikkinchi muhim chora — kuchli va noyob parollardan foydalanishdir. Har bir tizim uchun alohida parol ishlatilishi, parollar kamida 12–14 belgidan iborat bo‘lishi, ism, tug‘ilgan sana yoki telefon raqami kabi oson topiladigan ma’lumotlar qo‘llanmasligi kerak. Parol menejerlari ko‘plab murakkab parollarni xavfsiz saqlashga yordam beradi. Uchinchi chora — ko‘p faktorli autentifikatsiyadan foydalanishdir. MFA paroldan tashqari qo‘shimcha tasdiqlash omilini talab qiladi. Bunda autentifikator ilovasi, apparat xavfsizlik kaliti, biometrik tasdiqlash yoki passkey kabi usullar qo‘llanadi. SMS-kodlar ham foydali, lekin ular phishing va SIM-karta bilan bog‘liq firibgarlikka nisbatan zaifroq bo‘lishi mumkin. To‘rtinchi chora — havolalarni bosishdan oldin tekshirish. Shubhali xabardagi link orqali emas, balki brauzerga rasmiy sayt manzilini qo‘lda yozib kirish xavfsizroqdir. Masalan, bank, universitet portali yoki elektron pochta xizmatiga xabardagi havola orqali emas, rasmiy domen orqali kirish tavsiya etiladi. Beshinchi chora — qurilmalarni yangilab borish. Operatsion tizim, brauzer, antivirus, ofis dasturlari va mobil ilovalar muntazam yangilanmasa, phishing orqali yuborilgan zararli fayllar eski zaifliklardan foydalanishi mumkin. FTC ham qurilmalarni xavfsizlik dasturlari bilan himoyalash, avtomatik yangilash va muhim ma’lumotlarni zaxiralashni tavsiya qiladi.

Texnik himoya vositalari

Foydalanuvchi hushyorligi muhim bo‘lsa-da, tashkilot darajasidagi texnik himoya ham zarur. Elektron pochta filtrlari, spamga qarshi tizimlar, zararli havolalarni bloklash, DNS filtering, endpoint protection, antivirus va xavfsizlik devorlari phishingning bir qismini foydalanuvchiga yetib bormasdan to‘xtatadi. Elektron pochta domenlari uchun SPF, DKIM va DMARC sozlamalarini joriy etish muhim. SPF qaysi serverlar tashkilot nomidan xat yuborishi mumkinligini belgilaydi. DKIM xatga kriptografik imzo qo‘shadi. DMARC esa SPF va DKIM natijalariga asoslanib, soxta xatlar bilan qanday muomala qilishni ko‘rsatadi. Bu sozlamalar universitet yoki maktab nomidan soxta xat yuborilishini kamaytiradi. Kirish huquqlarini cheklash ham muhim tamoyildir. Har bir foydalanuvchiga faqat

o‘z vazifasi uchun zarur bo‘lgan huquqlar berilishi kerak. Agar oddiy foydalanuvchi akkaunti buzilsa, hujumchi butun tizimga kira olmasligi zarur. Bu “least privilege” tamoyili deb ataladi. Zaxira nusxalar ham phishing oqibatlarini kamaytiradi. Agar ransomware yoki zararli dastur fayllarni shifrlab qo‘ysa, to‘g‘ri tashkil etilgan zaxira nusxa orqali ma’lumotlarni tiklash mumkin bo‘ladi. Zaxira nusxalar muntazam sinovdan o‘tkazilishi va asosiy tarmoqdan alohida saqlanishi lozim.

O‘qituvchilar uchun amaliy tavsiyalar

O‘qituvchi phishingga qarshi kurashda ikki tomonlama rol bajaradi: bir tomondan, o‘z akkaunti va qurilmalarini himoya qiladi; ikkinchi tomondan, talabalarda xavfsiz raqamli odatlarni shakllantiradi. Shu sababli o‘qituvchi elektron pochta va ta’lim platformalaridan foydalanishda ehtiyotkor bo‘lishi kerak. Talabalardan kelgan kutilmagan fayllarni ochishdan oldin ularning manbasini tekshirish zarur. Agar fayl g‘alati formatda bo‘lsa yoki xabar matni odatiy uslubga mos kelmasa, talabadan boshqa kanal orqali tasdiq so‘rash kerak. Rasmiy hujjatlar va baholash materiallarini faqat tasdiqlangan platformalar orqali almashish tavsiya etiladi. Dars jarayonida phishing bo‘yicha qisqa amaliy topshiriqlar berish foydali. Masalan, talabalarga haqiqiy va soxta xabarlarni taqqoslash, domen nomidagi farqlarni aniqlash, shubhali havolani tekshirish yoki phishing xabarini xabar qilish tartibini ishlab chiqish vazifasi berilishi mumkin. Bu nazariy bilimni amaliy ko‘nikmaga aylantiradi.

Talabalar uchun amaliy tavsiyalar

Talabalar turli platformalar, messenjerlar, ijtimoiy tarmoqlar va onlayn xizmatlardan faol foydalanadi. Shu sababli ular har bir havola, xabar va faylga tanqidiy yondashishi kerak. Quyidagi qoidalar kundalik raqamli hayotda phishing xavfini kamaytiradi:

noma’lum havolalarni bosmaslik va rasmiy saytga bevosita kirish;

parol, SMS-kod, karta raqami yoki PIN-kodni hech kimga bermaslik;

universitet, bank yoki davlat portali nomidan kelgan xabarni rasmiy kanal orqali tekshirish;

bir xil parolni bir nechta saytga qo‘ymaslik;

grant, sovrin, stipendiya yoki bepul kurs haqidagi juda jozibali takliflarga ehtiyot bo‘lish;

telefon va noutbukda parol yoki biometrik himoya ishlatish;

begona Wi-Fi tarmoqlarida muhim akkauntlarga kirishda ehtiyotkor bo‘lish;

shubhali xabarni o‘qituvchi, IT mutaxassisi yoki mas’ul shaxsga ko‘rsatish.

Phishingga tushib qolish uyat emas; eng katta xato — buni yashirishdir. Vaqtida xabar berilsa, parol almashtiriladi, sessiyalar yopiladi, akkaunt tiklanadi va boshqa foydalanuvchilar ogohlantiriladi.

Phishingga tushib qolinsa bajariladigan choralar

Agar foydalanuvchi shubhali havolani bosgan, soxta sahifaga ma’lumot kiritgan yoki zararli faylni ochgan bo‘lsa, tezkor harakat qilish zarur. Quyidagi ketma-ketlik zarar miqdorini kamaytirishga yordam beradi:

internet aloqasini vaqtincha uzish yoki qurilmani tarmoqdan ajratish;

parolni faqat rasmiy sayt orqali almashtirish;

agar shu parol boshqa joylarda ham ishlatilgan bo‘lsa, ularni ham darhol yangilash;

elektron pochtadagi avtomatik yo‘naltirish va xavfsizlik sozlamalarini tekshirish;

bank ma’lumotlari kiritilgan bo‘lsa, bankka zudlik bilan murojaat qilish;

IT bo‘limi yoki mas’ul shaxsga xabar berish;

qurilmani antivirus va xavfsizlik vositalari bilan tekshirish;

akkauntdan yuborilgan zararli xabarlar bor-yo‘qligini tekshirish;

hodisadan keyin sabablarni tahlil qilib, takrorlanishining oldini olish.

2-jadval. Phishing hujumlarini aniqlashda foydalaniladigan tekshiruv mezonlari va tavsiya etiladigan himoya choralari

Tekshiruv savoli	Xavf belgisi	Tavsiya etiladigan amal
Xabar kutilmaganmi?	Ha, foydalanuvchi bunday xabarni kutmagan.	Yuboruvchini boshqa kanal orqali tekshirish.
Havola rasmiy domenga olib boryaptimi?	Domen nomi g‘alati yoki noto‘g‘ri yozilgan.	Havolani bosmaslik, saytga qo‘lda kirish.
Parol yoki kod so‘ralyaptimi?	Maxfiy ma’lumot talab qilinmoqda.	Ma’lumot bermaslik va xabar berish.
Shoshilinch bosim bormi?	“Darhol”, “24 soat ichida” kabi iboralar bor.	Shoshmasdan tekshirish.
Fayl kutilmaganmi?	Noaniq formatdagi ilova yuborilgan.	Ochmaslik, antivirusdan o‘tkazish.

Yuboruvchi shubhalimi?	Manzil yoki ism mos kelmaydi.	Rasmiy kontakt orqali aniqlashtirish.

Yuqoridagi jadvalda phishing hujumlarini aniqlashda foydalaniladigan asosiy tekshiruv mezonlari, ularning xavf belgilari hamda tavsiya etiladigan himoya choralari keltirilgan. Jadvaldan ko‘rinib turibdiki, phishing hujumlari ko‘pincha kutilmagan xabarlar yuborish, foydalanuvchini shoshilinch qaror qabul qilishga undash, soxta havolalar orqali maxfiy ma’lumotlarni qo‘lga kiritishga urinish va shubhali fayllarni tarqatish kabi usullar orqali amalga oshiriladi. Shu sababli foydalanuvchilar har qanday xabar yoki havolani ochishdan oldin uning manbasi va ishonchliligini tekshirishi zarur. Jadvalda ko‘rsatilgan tavsiyalar, jumladan yuboruvchini tasdiqlash, havolalarni tekshirish, maxfiy ma’lumotlarni taqdim etmaslik va antivirus vositalaridan foydalanish phishing xavfini sezilarli darajada kamaytirishga yordam beradi. Mazkur mezonlardan foydalanish ta’lim muassasalari hamda boshqa tashkilotlarda kiberxavfsizlik darajasini oshirish va foydalanuvchilarning raqamli savodxonligini mustahkamlashda muhim ahamiyat kasb etadi.

Xulosa

Phishing zamonaviy kiberxavfsizlikning eng dolzarb tahdidlaridan biri bo‘lib, u texnik vositalardan tashqari inson psixologiyasiga ham tayanadi. Hujumchilar foydalanuvchini qo‘rqitish, shoshiltirish, qiziqtirish yoki ishonchli tashkilot nomidan aldash orqali maxfiy ma’lumotlarni qo‘lga kiritishga harakat qiladi. Ta’lim muassasalari uchun phishing ayniqsa xavfli, chunki bu muhitda ko‘p sonli akkauntlar, shaxsiy ma’lumotlar, ilmiy ishlanmalar va rasmiy hujjatlar mavjud. Phishingni aniqlash uchun yuboruvchi manzili, havola, domen, xabar mazmuni, fayl ilovasi va shoshilinch talablar sinchiklab tekshirilishi kerak. Oldini olish esa kuchli parollar, ko‘p faktorli autentifikatsiya, xavfsiz elektron pochta sozlamalari, texnik filtrlar, doimiy treninglar va aniq xabar berish tartibiga asoslanadi. O‘qituvchilar va talabalar phishingga qarshi kurashda faol ishtirok etishlari zarur. Har bir foydalanuvchi “ishon, lekin tekshir” tamoyiliga amal qilishi, shubhali havolani bosmasligi, maxfiy ma’lumotlarni ulashmasligi va xatarni darhol mas’ul shaxslarga bildirishi kerak. Raqamli xavfsizlik madaniyati shakllangan ta’lim muassasasida phishing hujumlarining zararli oqibatlari sezilarli darajada kamayadi. Tahlillar shuni ko‘rsatadiki, phishing hujumlarining muvaffaqiyati ko‘pincha texnik zaifliklardan ko‘ra inson omili bilan bog‘liq. Shu sababli kiberxavfsizlikni ta’minlashda

foydalanuvchilarning raqamli savodxonligini oshirish eng muhim vazifalardan biri hisoblanadi. Kelgusida sun'iy intellekt texnologiyalarining rivojlanishi phishing xabarlarini yanada ishonchli ko'rinishga keltirishi mumkin. Shuning uchun tashkilotlar va foydalanuvchilar texnik himoya vositalari bilan bir qatorda doimiy o'qitish va profilaktik tadbirlarga ham alohida e'tibor qaratishlari zarur. Muallif fikricha, phishingga qarshi kurashning eng samarali usuli texnologik himoya va foydalanuvchi xabardorligini uyg'unlashtirishdan iborat.

Foydalanilgan adabiyotlar:

1. Cybersecurity and Infrastructure Security Agency (CISA). Recognize and Report Phishing.https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

2. Federal Trade Commission (FTC). How to Recognize and Avoid Phishing Scams. https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams

3. National Institute of Standards and Technology (NIST). Phishing Guidance for Cybersecurity. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

4. Anti-Phishing Working Group (APWG). Phishing Activity Trends Reports. https://apwg.org/trendreports

5. Microsoft Learn. Passkeys and Phishing-Resistant Authentication. https://learn.microsoft.com/en-us/entra/identity/authentication/concept authentication-passkeys-fido2

6. Jaxongir o'g'li, K. S., Nuriddinjon o'g'li, O. O., & Dilshodjon o'g'li, D. A. (2025). Ma'lumotlar bazasidan foydalanishda keng tarqalgan xatolar va ularni bartaraf etish. Education and Science Yesterday and Today, 1(1).

7. ENISA (European Union Agency for Cybersecurity). Phishing Threat Landscape. https://www.enisa.europa.eu/topics/csirt-cert-services/incident-handling/analysis/phishing

8. Verizon. Data Breach Investigations Report (DBIR). https://www.verizon.com/business/resources/reports/dbir/

9. Symantec (Broadcom). Internet Security Threat Report. https://www.broadcom.com/support/security-center/threat-reports

10. Cisco. Cybersecurity Awareness: Phishing Explained. https://www.cisco.com/c/en/us/products/security/what-is-phishinghtml