

PHISHING HUJUMLARI VA ZAMONAVIY HIMOYA USULLARI

Bo'riyev Shohjahon Sherzodovich

Toshkent viloyati O'rta chirchiq tumani 3-son texnikum, "Kampyuter grafikasi va dizayn operatorligi" yo'nalish talabasi

Annotatsiya: Ushbu maqolada kiberxavfsizlik sohasidagi eng dolzarb muammolardan biri bo'lgan phishing hujumlari va ularga qarshi zamonaviy himoya usullari yoritilgan. Maqolada phishing hujumlarining mohiyati, turlari, amalga oshirish mexanizmlari hamda ularning foydalanuvchilar va tashkilotlar uchun keltirib chiqaradigan salbiy oqibatlar batafsil tahlil qilingan. Shuningdek, phishing hujumlaridan himoyalaniishning foydalanuvchi darajasidagi, texnik va tashkiliy choralariga alohida e'tibor qaratilgan. Zamonaviy texnologiyalar, jumladan sun'iy intellekt va mashinaviy o'rganish asosida phishing hujumlarini aniqlash va oldini olish usullari ko'rib chiqilgan. Ushbu maqola kiberxavfsizlikka qiziquvchi talabalar va mutaxassislar uchun foydali manba bo'lib xizmat qiladi.

Kalit so'zlar: phishing hujumlari, kiberxavfsizlik, axborot xavfsizligi, ijtimoiy muhandislik, elektron pochta xavfsizligi, ikki bosqichli autentifikatsiya, sun'iy intellekt.

ФИШИНГОВЫЕ АТАКИ И СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ

Бურიев Шохжахон Шерзодович

Студент техникума № 3 Уртачирчикского района Ташкентской области, направление «Оператор компьютерной графики и дизайна»

Аннотация: В данной статье рассматривается одна из наиболее актуальных проблем в сфере кибербезопасности - фишинговые атаки и современные методы защиты от них. В статье подробно анализируются сущность фишинговых атак, их основные виды, механизмы реализации, а также негативные последствия для пользователей и организаций. Особое внимание уделяется пользовательским, техническим и организационным мерам защиты от фишинга. Кроме того, рассматривается применение современных технологий, таких как искусственный интеллект и машинное обучение, для выявления и предотвращения фишинговых атак. Статья может быть полезна студентам и специалистам, интересующимся вопросами кибербезопасности.

Ключевые слова: фишинговые атаки, кибербезопасность, информационная безопасность, социальная инженерия, безопасность электронной почты, двухфакторная аутентификация, искусственный интеллект.

PHISHING ATTACKS AND MODERN PROTECTION METHODS

Buriyev Shohjahon Sherzodovich

*Student of Technical College No. 3 of the O'rta Chirchiq District, Tashkent Region,
majoring in Computer Graphics and Design Operator*

Abstract: *This article examines one of the most pressing issues in the field of cybersecurity - phishing attacks and modern methods of protection against them. The paper provides a detailed analysis of the nature of phishing attacks, their main types, implementation mechanisms, and the negative consequences they pose to users and organizations. Special attention is given to user-level, technical, and organizational countermeasures against phishing. In addition, the use of modern technologies such as artificial intelligence and machine learning for detecting and preventing phishing attacks is discussed. This article serves as a useful resource for students and professionals interested in cybersecurity.*

Keywords: *phishing attacks, cybersecurity, information security, social engineering, email security, two-factor authentication, artificial intelligence.*

KIRISH

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi va internetdan foydalanishning kengayishi jamiyat hayotining barcha sohalariga chuqur kirib bormoqda[1]. Elektron pochta, ijtimoiy tarmoqlar, onlayn bank xizmatlari hamda masofaviy ish tizimlari kundalik hayotimizning ajralmas qismiga aylangan[6]. Ushbu qulayliklar bilan bir qatorda, axborot xavfsizligini ta'minlash masalasi ham dolzarb muammolardan biri sifatida namoyon bo'lmoqda.

Internet foydalanuvchilari sonining ortishi kiberjinoyatchilar uchun yangi imkoniyatlar yaratmoqda. Ayniqsa, foydalanuvchini aldash va uning ishonchidan foydalanishga asoslangan phishing hujumlari so'nggi yillarda eng keng tarqalgan kiberhujum turlaridan biriga aylandi[4],[5]. Phishing hujumlari orqali foydalanuvchilarning shaxsiy ma'lumotlari, login va parollari, bank karta ma'lumotlari noqonuniy ravishda qo'lga kiritilmoqda[9].

Phishing hujumlarining xavfliligi shundaki, ular ko'pincha murakkab texnik bilimlarni talab qilmaydi, balki inson omiliga - ya'ni foydalanuvchining e'tiborsizligi va yetarli bilimga ega emasligidan foydalanadi. Hujumchilar banklar, mashhur kompaniyalar yoki davlat tashkilotlari nomidan soxta xabarlar yuborib, foydalanuvchini zararli havolalarga yo'naltiradi yoki maxfiy ma'lumotlarini kiritishga majbur qiladi. Natijada esa katta moliyaviy zararlar va axborot yo'qotish holatlari yuzaga keladi.

So'nggi yillarda phishing hujumlari yanada murakkablashib, sun'iy intellekt, ijtimoiy muhandislik va avtomatlashtirilgan texnologiyalar yordamida amalga oshirilmoqda. Bu esa phishing hujumlariga qarshi zamonaviy himoya usullarini qo'llash zaruratini oshirmoqda. Shu sababli phishing hujumlarining mohiyatini o'rganish, ularning turlari, ishlash mexanizmlari va himoyalash usullarini tahlil qilish kiberxavfsizlik sohasidagi muhim vazifalardan biri hisoblanadi.

Mazkur maqolada phishing hujumlarining tushunchasi va tarixiy rivojlanishi, asosiy turlari, amalga oshirish mexanizmlari, keltirib chiqaradigan oqibatlari hamda

zamonaviy himoya usullari keng yoritiladi. Maqolaning asosiy maqsadi phishing hujumlari haqida aniq tushuncha berish va kiberxavfsizlikni ta'minlash bo'yicha foydali tavsiyalar ishlab chiqishdan iborat.

1. Phishing hujumlari tushunchasi va tarixiy rivojlanishi: Phishing atamasi ingliz tilidagi "fishing" so'zidan kelib chiqqan bo'lib, foydalanuvchini aldash orqali maxfiy ma'lumotlarni qo'lga kiritishni anglatadi[3]. Atamadagi "ph" harflari esa dastlab telefon tizimlarini buzish bilan shug'ullangan phreaking tushunchasidan olingan.

Phishing hujumlarining dastlabki ko'rinishlari 1990-yillarda paydo bo'lgan. O'sha davrda hujumlar asosan elektron pochta va onlayn xizmatlar orqali amalga oshirilgan bo'lib, foydalanuvchilarning login va parollarini qo'lga kiritishga qaratilgan edi[1],[2].

Bugungi kunda phishing hujumlari yanada murakkablashib, SMS, telefon qo'ng'iroqlari, ijtimoiy tarmoqlar va soxta veb-saytlar orqali amalga oshirilmoqda. Zamonaviy texnologiyalar, jumladan sun'iy intellektdan foydalanilishi bu hujumlarni aniqlashni yanada qiyinlashtirmoqda[4],[8]. Shu sababli phishing hujumlari kiberxavfsizlik sohasidagi eng dolzarb tahdidlardan biri hisoblanadi.

2. Phishing hujumlarining asosiy turlari: Phishing hujumlari amalga oshirilish usuliga qarab bir nechta asosiy turlarga bo'linadi. Ushbu hujum turlari foydalanuvchini aldash va maxfiy ma'lumotlarni qo'lga kiritishga qaratilgan bo'lib, ular turli aloqa kanallari orqali amalga oshiriladi.

Email phishing - eng keng tarqalgan phishing turi hisoblanadi. Bu usulda hujumchilar banklar, kompaniyalar yoki mashhur xizmatlar nomidan soxta elektron xatlar yuborib, foydalanuvchini zararli havolalarga o'tishga yoki maxfiy ma'lumotlarini kiritishga majbur qiladi[5],[6].

Spear phishing - aniq bir shaxs yoki tashkilotga yo'naltirilgan hujum bo'lib, hujumchi jabrlanuvchi haqida oldindan ma'lumot to'plagan holda ishonchli xabar tayyorlaydi. Bu turdagi hujumlar odatda yirik tashkilotlar va rahbar xodimlarga qaratiladi ya'ni aniq bir shaxs yoki tashkilotga qaratilgan hujum bo'lib, hujumchi oldindan to'plangan ma'lumotlarga asoslanadi [2],[9].

Smishing - SMS xabarlar va telefon qo'ng'iroqlari orqali amalga oshiriladigan phishing hujumidir[5],[8]. Bunda foydalanuvchiga bank yoki xizmat ko'rsatuvchi tashkilot nomidan qisqa xabar yuborilib, havolaga o'tish yoki ma'lumotlarni kiritish so'raladi.

Vishing - telefon qo'ng'iroqlari orqali amalga oshiriladigan phishing hujumi bo'lib, hujumchi o'zini bank yoki texnik yordam xodimi sifatida tanishtiradi va foydalanuvchidan maxfiy ma'lumotlarni olishga harakat qiladi[5],[8].

Soxta veb-saytlar orqali hujumlar - haqiqiy sayt dizayniga juda o'xshash sahifalar yaratiladi. Foydalanuvchi ushbu saytlarga kirib login va parolini kiritganda, ma'lumotlar to'g'ridan-to'g'ri hujumchiga uzatiladi[10].

3. Phishing hujumlarining ishlash mexanizmi: Phishing hujumlari odatda bir necha ketma-ket bosqichlarda amalga oshiriladi. Dastlab hujumchi jabrlanuvchini tanlaydi va unga ishonch uyg'otuvchi soxta xabar yoki havola tayyorlaydi. Keyingi bosqichda foydalanuvchi ushbu xabar orqali zararli havolaga o'tadi yoki maxfiy ma'lumotlarini

kiritadi. Oxirgi bosqichda esa hujumchi olingan ma'lumotlardan noqonuniy maqsadlarda foydalanadi[3].

Ijtimoiy muhandislik usullari phishing hujumlarining asosini tashkil etadi. Hujumchilar foydalanuvchining ishonuvchanligi, qo'rquvi yoki shoshilinch qaror qabul qilish holatidan foydalanadi. Masalan, "akkauntingiz bloklandi" yoki "zudlik bilan tasdiqlang" kabi xabarlar foydalanuvchini chalg'itadi[9],[4].

Foydalanuvchini aldash texnikalariga soxta tashkilot nomidan murojaat qilish, real veb-saytlarga o'xshash sahifalar yaratish va ishonarli dizayndan foydalanish kiradi. Ushbu usullar orqali foydalanuvchi o'z ma'lumotlarini o'zi bilmagan holda hujumchiga taqdim etadi.

4. Phishing hujumlarining oqibatlari va xavf darajasi: Phishing hujumlari foydalanuvchilar va tashkilotlar uchun jiddiy salbiy oqibatlarga olib keladi. Eng asosiy oqibatlardan biri - moliyaviy zararlar bo'lib, bank hisoblaridan mablag'larning noqonuniy yechib olinishi yoki to'lov ma'lumotlarining o'g'irlanishi bilan bog'liq[1],[5].

Shuningdek, phishing hujumlari natijasida shaxsiy ma'lumotlar yo'qotiladi. Login, parol va boshqa maxfiy ma'lumotlarning oshkor bo'lishi foydalanuvchi akkauntlarining buzilishiga sabab bo'ladi.

Tashkilotlar uchun esa phishing hujumlari obro'ga putur yetkazishi, mijozlar ishonchining pasayishi va katta moliyaviy yo'qotishlarga olib kelishi mumkin. Shu sababli phishing hujumlari kiberxavfsizlikka jiddiy tahdid hisoblanadi[2],[6].

5. Zamonaviy phishing hujumlari va yangi tahdidlar: So'nggi yillarda phishing hujumlari zamonaviy texnologiyalar yordamida yanada murakkablashmoqda. Sun'iy intellekt asosida yaratilgan xabarlar ishonarli matn va dizayn orqali foydalanuvchini tezroq chalg'itadi[9].

Deepfake texnologiyalari yordamida soxta ovoz va video yaratilib, foydalanuvchidan maxfiy ma'lumotlarni olishga urinish holatlari ko'paymoqda[9]. Bundan tashqari, avtomatlashtirilgan hujumlar katta miqdordagi foydalanuvchilarga qisqa vaqt ichida phishing xabarlarini yuborish imkonini beradi[4].

Ushbu tahdidlar phishing hujumlariga qarshi zamonaviy va kompleks yondashuvlarni qo'llash zarurligini ko'rsatadi.

6. Phishing hujumlaridan himoyalaniş usullari: Phishing hujumlaridan samarali himoyalaniş uchun foydalanuvchi, texnik va tashkiliy darajadagi choralarni birgalikda qo'llash zarur.

Foydalanuvchi darajasidagi himoya shubhali xabar va havolalarga bosmaslik, jo'natuvchini tekshirish, kuchli parollardan foydalanish hamda ikki bosqichli autentifikatsiyani yoqishni o'z ichiga oladi[9].

Texnik himoya vositalari sifatida antivirus dasturlari, anti-phishing filtrlari, email xavfsizlik tizimlari va brauzer himoya vositalaridan foydalaniladi. Ushbu vositalar zararli xabarlarni aniqlash va bloklashga yordam beradi[10].

Tashkiliy va boshqaruv choralari esa xodimlarni kiberxavfsizlik bo'yicha muntazam o'qitish, xavfsizlik siyosatlarini joriy etish hamda nazorat va monitoring tizimlarini tashkil etishni o'z ichiga oladi[2].

7. Phishingga qarshi zamonaviy texnologiyalar: Bugungi kunda phishing hujumlarini aniqlash va oldini olishda sun'iy intellekt (AI) va mashinaviy o'rganish (Machine Learning) texnologiyalaridan keng foydalanilmoqda[7]. Ushbu tizimlar shubhali xabarlar, havolalar va foydalanuvchi xatti-harakatlarini tahlil qilib, phishing hujumlarini aniqlaydi[10].

Real vaqt monitoringi orqali tizimlar xavfli faoliyatni tezkor aniqlab, hujumlarning oldini olishga yordam beradi. Bu esa kiberxavfsizlik darajasini oshirib, foydalanuvchilar va tashkilotlar uchun samarali himoya ta'minlaydi.

Xulosa: phishing hujumlari hozirgi kunda kiberxavfsizlik sohasidagi eng keng tarqalgan va xavfli tahdidlardan biri hisoblanadi[1],[4]. Ushbu hujumlar asosan foydalanuvchini aldash va uning e'tiborsizligidan foydalanish orqali amalga oshiriladi. Natijada moliyaviy zararlar, shaxsiy ma'lumotlarning yo'qotilishi hamda tashkilotlar obro'siga putur yetishi mumkin.

Phishing hujumlaridan samarali himoyalani uchun faqat texnik vositalar yetarli emas. Foydalanuvchilarning kiberxavfsizlik bo'yicha bilim va ongini oshirish, shubhali xabar va havolalarga nisbatan ehtiyotkor bo'lishi muhim ahamiyatga ega. Shuningdek, antivirus dasturlari, ikki bosqichli autentifikatsiya va zamonaviy xavfsizlik tizimlaridan foydalanish himoya darajasini oshiradi[7],[9].

Kelajakda phishing hujumlari yanada murakkablashishi kutilmoqda, chunki sun'iy intellekt va avtomatlashtirilgan texnologiyalar hujumchilar tomonidan ham qo'llanilmoqda. Shu sababli kiberxavfsizlik sohasida zamonaviy yondashuvlar, real vaqt monitoringi va AI asosidagi himoya tizimlarini joriy etish muhimdir. Faqatgina kompleks va ongli yondashuv orqali phishing hujumlarining oldini olish mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. Stallings, W. Network Security Essentials: Applications and Standards. Pearson Education, 2021. (Phishing hujumlari tushunchasi va tarmoq xavfsizligi asoslari)
2. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020. (Kiberxavfsizlik va hujum mexanizmlari)
3. Mitnick, K., Simon, W. The Art of Deception: Controlling the Human Element of Security. Wiley Publishing, 2019. (Ijtimoiy muhandislik va foydalanuvchini aldash usullari)
4. ENISA (European Union Agency for Cybersecurity). Phishing Threat Landscape. Internet manbasi. (Phishing hujumlarining turlari va zamonaviy tahdidlar)
5. Kaspersky Lab. Phishing Attacks: Types, Examples and Protection Methods. Internet manbasi. (Email phishing, smishing, vishing va himoya usullari)
6. Cisco Systems. Email Security and Phishing Attacks Overview. Internet manbasi. (Texnik himoya vositalari)
7. IBM Security. Artificial Intelligence and Machine Learning in Cybersecurity. Internet manbasi. (AI va Machine Learning asosidagi himoya tizimlari)
8. Cloudflare. What is Phishing and How to Prevent It?

Internet manbasi. (Phishing hujumlaridan himoyalanish usullari)

9. Microsoft Security. Phishing and Social Engineering Attacks.

Internet manbasi. (Foydalanuvchi va tashkiliy darajadagi himoya)

10. OWASP Foundation. Phishing Attack Prevention Guide. Internet manbasi.
(Zamonaviy yondashuvlar va real vaqt monitoringi)