FISHING HUJUMLARDAN HIMOYA QILISHNING ASOSIY USULLARI VA CHORALARI

Abdumuxtor Umarov
TATU Farg'ona filiali katta o'qituvchisi
Turdimatova Qutlug'beka
TATU Farg'ona filiali talabasi

Annotatsiya: *Maqolada kibertahdidlarning eng keng tarqalgan turlaridan biri bo'lgan fishing hujumlaridan himoyalanishning asosiy usullari va strategiyalari ko'rib chiqiladi. Bu foydalanuvchilarni aldash va maxfiy ma'lumotlarni olish uchun tajovuzkorlar tomonidan qo'llaniladigan fishing usullarini tavsiflaydi. Maqolada xavflarni minimallashtirish va potentsial hujumlardan himoya qilish uchun asosiy vositalar va xavfsizlik choralari keltirilgan.*

Kalit so'zlar: *Fishing hujumlari, kiberxavfsizlik, himoya usullari, aldash, foydalanuvchi ma'lumotlari, xavfsizlik choralari, axborot xavfsizligini ta'minlash.*

Abstract: *The article examines the main methods and strategies for protecting against phishing attacks, one of the most common types of cyberthreats. It describes phishing techniques used by attackers to trick users and obtain confidential information. The article provides basic tools and security measures to minimize risks and protect against potential attacks.*

Keywords: *Phishing attacks, cyber security, protection methods, fraud, user data, security measures, information security.*

Fishing - bu ijtimoiy muhandislik tamoyillari asosida qurilgan Internetdagi firibgarlikning bir turi. Fishingning asosiy maqsadi muhim ma'lumotlar (masalan, pasport ma'lumotlari), hisoblar, bank rekvizitlari va maxfiy mulkiy ma'lumotlardan kelajakda pul o'g'irlash uchun foydalanish uchun kirishdir. Fishing foydalanuvchilarni haqiqiy manbalarga to'liq taqlid qiluvchi soxta tarmoq resurslariga yo'naltirish orqali ishlaydi.

Barcha fishing hujumlarining aksariyati ushbu toifaga kiradi. Buzg'unchilar foydalanuvchi hisob ma'lumotlarini tortib olish va shaxsiy yoki biznes hisoblarini nazorat qilish uchun haqiqiy kompaniya nomidan elektron pochta xabarlarini yuborishadi. Siz to'lov tizimi yoki bank, yetkazib berish xizmati, onlayn-do'kon, ijtimoiy tarmoq, soliq idorasi va boshqalar nomidan fishing elektron pochta xabarini olishingiz mumkin.

Bunday xatlardagi havolani bosish uchun ("Agar siz 24 soat ichida ro'yxatdan o'tgan bo'lsangiz, xizmatlarga 70% chegirma olishingiz mumkin") yoki ("hisobingiz quyidagi sabablarga ko'ra bloklangan"),(hisob egasi ekanligingizni tasdiqlash uchun havolaga o'ting") kabi gaplar bilan chalg'itish mumkin.

Quyida firibgarlarning eng mashhur hiylalari ro'yxati bilan tanishib chiqamiz:

- Hisobingizda shubhali yoki firibgarlik harakati aniqlandi. Xavfsizlik sozlamalarini yangilash kerak.

Bunday xatda foydalanuvchidan zudlik bilan o'z akkauntiga kirish va xavfsizlik sozlamalarini yangilash so'raladi. Xuddi shu printsip avvalgi bandda bo'lgani kabi qo'llaniladi. Foydalanuvchi vahima qiladi va hushyor bo'lishni unutadi.

- Siz muhim xabar oldingiz. Uni tekshirish uchun shaxsiy hisobingizga o'ting.

Ko'pincha bunday xatlar moliya tashkilotlari nomidan yuboriladi. Foydalanuvchilar elektron pochta xabarlarining to'g'riligiga ishonishadi, chunki moliyaviy institutlar aslida elektron pochta orqali nozik ma'lumotlarni jo'natmaydi.

- Soliq bilan bog'liq fishing elektron pochta xabarlari va boshqalar.

Ushbu resurslardagi hisoblarga kirish tajovuzkorlar uchun jozibali istiqbol bo'lishi ajablanarli emas. Ushbu maqsadga erishish uchun standart yondashuv qo'llaniladi.

Fishingdan himoya qilish - asosiy qoidalar

1. Kichik imlo xatolari uchun tavsiya etilgan URL manzilini tekshiring.
2. Faqat xavfsiz https ulanishlaridan foydalaning. Sayt manzilida faqat bitta "s" harfining yo'qligi qizil bayroqlarni ko'tarishi kerak.
3. Qo'shimchalari yoki havolalari bo'lgan har qanday elektron pochta xabarlariga shubha qiling. Agar ular tanish manzildan kelgan bo'lsa ham, bu xavfsizlikni kafolatlamaydi: u buzilgan bo'lishi mumkin.
4. Agar siz kutilmagan shubhali xabarni olsangiz, jo'natuvchiga boshqa yo'l bilan murojaat qilishingiz va u yuborgan yoki yubormaganligini bilib olishingiz kerak.
5. Onlayn banking va boshqa moliyaviy xizmatlarga kirish uchun ochiq Wi-Fi tarmoqlaridan foydalanmang: ular ko'pincha tajovuzkorlar tomonidan yaratilgan. Bunday bo'lmasa ham, himoyalanmagan ulanishga ulanish xakerlar uchun qiyin emas.
6. Barcha hisoblarda, iloji bo'lsa, ikki faktorli autentifikatsiyani yoqing. Agar asosiy parol xakerlarga ma'lum bo'lsa, ushbu chora vaziyatni

saqlab qolishi mumkin.

Xulosalar

Yaqin kelajakda fishing butunlay yo'q qilinishi dargumon: bunga insonning dangasaligi, ishonuvchanligi va ochko'zligi sabab bo'ladi.

Har kuni minglab fishing hujumlari sodir bo'ladi, ular turli shakllarda bo'lishi mumkin:

- Klassik fishing.
- Maqsadli fishing hujumi.
- Yuqori boshqaruvga qarshi fishing.
- Google va Dropbox'dan fishing elektron pochta xabarlari.
- Biriktirilgan fayllar bilan fishing elektron pochta xabarlari.
- Pharming.

Mahalliy kompyuter yoki tarmoq uskunasida DNS keshini o'zgartirish orqali firibgar saytga yashirin yo'naltirish.

Shuning uchun, fishingga qarshi qoidalarni o'qib chiqing. Va eng muhimi, parollaringizni hech kimga bermang, har doim kerakli saytlarning manzillarini qo'lda kiritish yoki brauzeringizda xatcho'plardan foydalanishni odat qiling, ayniqsa shubxali havolalardan ehtiyot bo'ling.

FOYDALANILGAN ADABIYOTLAR.

1. Umarov, A. (2023). Bulutli ma’lumotlarni himoya qilish: ma’lumotlar xavfsizligini ta’minlash. Conference on Digital Innovation : "Modern Problems and Solutions".

2. Umarov, A. (2023). Axborotni ruxsatsiz kirishdan himoya qilish texnologiyalarini ishlab chiqish. Conference on Digital Innovation : "Modern Problems and Solutions".

3. Umarov, A. (2023). Axborotni ruxsatsiz foydalanishdan himoya qilishda foydalanuvchilarni o’qitish va xabardorlikning roli. Conference on Digital Innovation : "Modern Problems and Solutions".

4. Umarov, A. (2023). Axborotni ichki tahdidlardan himoya qilish: ruxsatsiz foydalanishning oldini olish. Conference on Digital Innovation : "Modern Problems and Solutions".

5. Umarov, A. (2023). Axborotni ruxsatsiz kirishdan himoya qilishda audit va monitoringning roli. Conference on Digital Innovation : "Modern Problems and Solutions".

6. Umarov, A. (2023). Xavfsizlik hodisalari: profilaktika choralari va ma’lumotlardan ruxsatsiz foydalanishga qarshi choralar. Conference on Digital Innovation : "Modern Problems and Solutions"

7. Makhmudov, I. A., & Isroiljonova, G. S. (2021). The package multiservice services in NGN. Academic research in educational sciences, 2(6), 989-994.

8. To‘ychiboyevich, K. S., & Saminjonovna, I. G. (2023). YURAK URISH TEZLIGINING OZGARUVCHANLIGINI ORGANISH. INNOVATION IN THE MODERN EDUCATION SYSTEM, 3(30), 389-395.

9. Abdumalikjon Vahobjon, Umarov , A., & Qodirov Ahmadxon. (2023). PYTHONDA ARRAYLAR, MASSIVLAR, MATRITSALAR VA NUMPY KUTUBXONASI IMKONIYATLARI. Educational Research in Universal Sciences, 2(12), 327–329.

10. Umarov, A., & Ro‘zaliyev, A. (2023). AXBOROTNI RUXSATSIZ FOYDALANISHLARDAN HIMOYALASH. Educational Research in Universal Sciences, 2(11), 500–502

11. Umarov, A., & Mirzayev, J. (2023). Next-Generation Firewalls: Enhancing Network Security in the Digital Era. Conference on Digital Innovation : "Modern Problems and Solutions".

12. Ro‘zaliyev Abdumalikjon Vahobjon o’g’li, Umarov Abdumuxtor Maxammad o‘g‘li, & R. Adaxanov. (2022). AXBOROT XAVFSIZLIGIDA BIOMETRIK HIMOYA USULLARI. Proceedings of International Educators Conference, 1(2), 177–181.

13. Muxtorov Farrux Muxammadovich, Umarov Abdumuxtor Maxammad o’g’li, & Ro’zaliyev Abdumalikjon Vahobjon o’g’li. (2022). AXBOROTNI XIMOYALASH

14. Умаров , А. (2023). ПРОЕКТНАЯ МЕТОДИКА В ПРЕПОДАВАНИИ КРИПТОГРАФИИ: РАЗВИТИЕ ТВОРЧЕСКИХ И КОММУНИКАТИВНЫХ НАВЫКОВ. Conference on Digital Innovation : "Modern Problems and Solutions".

15. Умаров , А. (2023). ИНТЕГРИРОВАННЫЙ ПОДХОД К ПРЕПОДАВАНИЮ КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ В ВУЗАХ: ТЕОРИЯ И ПРАКТИКА. Conference on Digital Innovation : "Modern Problems and Solutions".