

FISHING - GLOBAL XAVF

Abdujabborov Akbarali Toxirjon o'g'li

To'lanboyev Orifjon Ibrohimjon o'g'li

akbarinsta05@gmail.com

<https://doi.org/10.5281/zenodo.15212124>

Annotatsiya. Mazkur maqolada XXI asr boshlarida paydo bo'lgan va rivojlangan axborot texnologiyalari davrida internet foydalanuvchilari uchun xavfli tuzoqqa aylanib borayotgan fishing haqida so'z yuritiladi. Fishing kelib chiqish tarixi, rivojlanib borish omillari, yetkazayotgan zararlari va fishingga qarshi kurashish usullari haqida fikr mulohazalar bildirilgan.

Kirish so'zlar: fishing, kiber jinoyatlar, firibgarlik sxemalari, ideal yechim.

PHISHING-GLOBAL RISK

Abstract. This article talks about phishing, which appeared at the beginning of the 21st century and is becoming a dangerous trap for Internet users in the era of advanced information technologies. The history of the origin of phishing, the factors of its development, the harm it causes, and the methods of combating phishing are discussed.

Keywords: phishing, cyber crimes, fraud schemes, ideal solution.

РЫБАЛКА – ГЛОБАЛЬНАЯ УГРОЗА

Аннотация. В данной статье рассматривается фишинг, возникший в начале XXI века и становящийся опасной ловушкой для пользователей сети Интернет в эпоху передовых информационных технологий. Высказываются мнения об истории фишинга, факторах, способствующих его развитию, причиняемом им вреде и методах борьбы с фишингом.

Ключевые слова: фишинг, киберпреступность, мошеннические схемы, идеальное решение.

KIRISH

Allaqachon rivojlangan texnologiyalar asriga aylanib bo'lgan XXI asrda takkomillashgan mexanizmlar, insoniyat hayoti uchun foyda keltirgan raqamli texnologiyalar bilan bir qatorda ushbu axborot texnologiyalari va internet tarmoqlaridan foydalanuvchilar uchun xavfli bo'lgan turli xil xavfli saytlar, kiber jinoyatlar ham rivojlanib bormoqda.

Xususan fishing bu kiber jinoyat bo'lib, turli xil qonuniy faoliyat yurutayotgan muassalar sifatida elektron pochta, SMS xabarnomalar yoki telefon orqali shaxslarning shaxsiy ma'lumotlari: bank, kredit karta va parollar yoki passport seriya raqamlari kabi maxfiy ma'lumotlarini taqdim etishlari uchun shaxslarga bog'lanib, olgan ma'lumotlaridan ularning moliyaviy holati uchun xavfli bo'lgan jinoyatlar sodir etishda foydalanadilar.

MUHOKAMA VA TAHLIL

Ilk bor fishing jinoyati 2004-yilda "Amerika Online" veb-saytiga taqlid qilgan Kaliforniyalik o'smirga nisbatan qo'zg'atilgan. Ushbu soxta veb-sayt orqali sayt foydalanuvchilarining shaxsiy ma'lumotlarini olishga va ularning hisobidan pul undurish uchun kredit karta ma'lumotlariga kirishga muvaffaq bo'ldi.

Keyinchalik texnologiya va internet tarmoqlari rivojlanishi oqibatida fishingning ham xavfli ta'sir doirasi kengayib bordi va Fishingning o'zi bir necha guruhlariga bo'linib bordi:

1. Spir phishing- fribgarlar nishonga olingan shaxsga xuddi unga yaqin kishisi (hamkasbi yoki do'sti) tomonidan yuborilgandek ko'rinadigan elektron pochta, SMS, ijtimoiy tarmoqlar orqali yuborilgan xabarli matnlar ko'rinishida bo'ladi.

2. Veyling hujumlari- bu fishing turi "katta o'ljaga" qaratilgan bo'ladi ya'ni yuqori davlat amaldorlari yoxud korxona, muassasa tomonidan korxona, muassasa va tashkilot rahbarlarini yoki shu kabi mansabdor shaxslarga yuboriladigan elektron pochta xabarlari ko'rinishida bo'ladi.

3. SMishing- SMS xabarlar orqali amalga oshiriladigan fishing turi hisoblanadi. SMS yuboruvchi sizga pul yoki shaxsiy ma'lumotlaringizni olish uchun o'zini tanish qilib ko'rsatishlari mumkin.

4. Vishing- bu telefon orqali amalga oshiriladigan fishing turi. Bunday fishing turi bilan shug'ullanuvchi fribgarlar o'zlarini davlat idoralari xodimlari sifatida ko'rsatishadi, tahdid va ishontirish usullaridan foydalanishadi.

Fishingning turlari bilan tanishar ekanmiz bu jinoyat turi manipulyatsiya orqali kishilarning his-tuyg'ularidan foydalangan holda qurbon qilishini ko'rishimiz mumkin. Misol uchun, kishidagi qiziqqonlik, qo'rquv, ochko'zlik va shoshilinchlik. Bular kishilarni yetarlicha mulohaza va tahlil qilmay qaror qabul qilishiga olib keladi.

Afsuski, bu jinoyat soni kundan kunga oshib bormoqda xususan har bir fishing hujumida o'rtacha 136 dollar yo'qotilgan bo'lsa, bu 2021-yilda kiber jinoyatchilar tomonidan fishing hujumlari orqali o'g'irlangan 44,2 million dollarni tashkil etadi.

Shuningdek, 2024-yil mart oyi statistikasiga ko'ra har kuni 3,4 milliard spam xatlari yuboriladi, Google har kuni 100 millionga yaqin fishing xatlarini bloklaydi.

Bugungi kunga kelib O'zbekistonda ham ushbu jinoyat soni keskin oshib bormoqda. Bu borada O'zbekiston Respublikasi Kibrxavfsizlik markazining bergan ma'lumotlariga qaraydigan bo'lsak, mamlakatimizda fishingning keng tarqalgan turlaridan biri veb-saytlarni soxtalashtirish ya'ni turli xil veb- saytlar orqali foydalanuvchilarni chuv tushurish holatlari keng kuzatilmoqda.

Jumladan, www.President-uz, turli tashkilot va banklarning rasmiy veb-saytlarini qalbakilashtirish avj oldi. Statistika qaraydigan bo'lsak, "Kibrxavfsizlik markazi" davlat unitar korxonasi tomonidan joriy 2022-yil mobaynida moliyaviy firibgarlik bilan bog'liq bo'lgan 39 ta fishing veb-sahifalar aniqlandi va faoliyati tegishli tartibda O'zbekiston Respublikasi hududida cheklandi.

Fishing yetkazadigan zararlar haqida alohida to'xtalib o'tadigan bo'lsak, yuqorida keltirilga fishing turlari haqidagi ma'lumotlardan ko'rinib turibiki fishing jismoniy va yuridik shaxslarning konstitutsiyaviy huquqlaridan biri bo'lgan shaxsiy hayotning daxlsizligi huquqini buzilishiga, shuningdek shaxslarning moddiy va ma'naviy zarar ko'rishiga olib kelmoqda.

O'zbekiston Respublikasi konstitutsiyasining 31-moddasida har bir insoning shaxsiy hayotning daxlsizligi, shaxsiy sirga ega bo'lish, yozishmalari, telefon orqali so'zlashuvlari, shuningdek pochta, electron va boshqa xabarlar sir saqlanishi huquqiga ega ekanligi ta'kidlab o'tilgan. Kiberjinoyatning keng tarqalgan turi hisoblangan fishing esa shaxsning ushbu huquqlarining qo'pol tarzda buzulishidir. Konstitutsiyaviy huquqlarning buzulishi esa O'zbekiston Respublikasi Jinoyat kodeksining 7- bobi manashu konstitutsiyaviy huquqlarning buzilishiga bag'ishlangan, 141¹-moddasi esa aynan shaxsiy hayotning daxlsizliginni buzganligi uchun sanksiya qismi belgilangan. Bu esa ushbu huquqning qay darajada himoyalanganligini bildirsada, sodir bo'layotgan fishing jinoyatlarining soni kamayishiga yordam berolmayapti.

Butun dunyo bo'ylab fishingni oldini olish har kuni insonlarni ogohlikka chaqiruvlar, ogohlantirishlar, turli xil jurnal va TV ko'rsatuvlar orqali ogohlantirib borilmoqda. Xususan, mamlakatimizda ham aholini ogohlikka chaqirish uchun "Kibrxavfsizlik markazi" davlat unitar korxonasi, O'zbekiston Respublikasi Markaziy banki tomonidan rasmiy bayonotlar, fishingga doir ma'lumotlar, fishingning oldini olishga qaratilgan tadbirlar amalga oshirilmoqda. Misol qilib olishimiz mumkinki, O'zbekiston Respublikasi Markaziy banki tomonidan "Moliyaviy bilim" loyihasi doirasida hozirgi kunda keng tarqalgan firibgarlik va uning turlari haqida videorolik va ma'lumotlar tayyorlandi.

O‘zbekistondagi eng katta firibgarlik sxemalari bular fishingning yuqorida keng tarqalgan 4 turi bo‘yicha eng keng tarqalgan firibgarlik turlaridir. Bular “Katta meros”, “Sovrinli yutuq”, “Telegram piramidasi” kabilardir.

“Kasalni davolagandan ko‘ra uning oldini olish kerak” degan naql bor xalqimizda shu tufayli ham Xalqaro dunyo hamjamiyati ekspertlar va bu soha vakillari aholini ogohlikka chaqirish aldanib qolmasliklari uchun qator tavsiyalar berib borilmoqda:

Saytlardan foydalanganda ularning URL manziliga e‘tiborli bo‘lib foydalangan maqsadga muvofiq hisoblanadi. Foydalanuvchilarga agar sayt haqida biror bir shubha tug‘ilgan taqdirda uni Norton Safe Web (<https://safeweb.norton.com>) kabi havola skaneri bilan skanerlash orqali tekshirib ko‘rish, qisqartirilgan URL havolalardan foydalanishda esa o‘ta ehtiyot bo‘lish, qisqartirilgan havola ortidagi haqiqiy URL havolasini tekshirish uchun UnshortenIt (<https://unshorten.it>) kabi bepul onlayn xizmatdan foydalanish doimiy tarzda aytib ogohlikka chaqirib kelinmoqda.

Shuningdek, Fishing hujumlarini amalga oshirish uchun ommaviy elektron pochtdan foydalanadigan firibgarlar ko‘pincha o‘nlab turli mamlakatlardagi odamlarni birdaniga nishonga oladi. Ular xabarlarini tarjima qilish va mahalliy auditoriya uchun moslashtirishga sarmoya sarflamaydilar, shunchaki bepul onlayn tarjima xizmatlaridan foydalanadilar. Natijada, fishing elektron pochta xabarlari ko‘pincha g‘ayritabiiy yoki g‘alati tilda va g‘ij-g‘ij grammatik xatolarga to‘la bo‘ladi.

«Kimga» maydonida shaxs ismi o‘rnida umumiy murojaat elektron pochta xabarining “Hurmatli mijoz”, “Hurmatli hisob egasi”, “Hurmatli klub a‘zosi” kabi umumiy murojaat bilan boshlanishi kishida doim shubha uyg‘otishi kerak. Mijozlar bilan bog‘lanuvchi haqiqiy tashkilotlar ko‘pincha mijozining ismi-sharfini kabi oddiy ma‘lumotlarga ega bo‘ladi.

Biroq chaqiriqlar va ogohlantirishlarga qaramay aholi orasida fishingning ulkan to‘riga tushib qolib aziyat chekayotganlar soni nafaqat O‘zbekistonda balki butun dunyo bo‘ylab ortib bormoqda.

XULOSA

Xulosa qilib aytganda, fishing XXI asr uchun hali to‘liq da‘vosi topilmagan yuqumli virus ko‘rinishidagi “kassallikdir”. Bu “kasallika” chalinmaslik uchun har kim o‘zida unga qarshi imunitet shakllantirishi zarur. Zero, xalqimizda “O‘zingni ehtiyot qil, qo‘shningni o‘g‘ri tutma”, degan naql bejizga emas. Ogohlik davr talabiga aylangan bir paytda har bir shaxsni hushyorlikka chaqiramiz va bunga bepisantlik qilmasliklarini so‘rab qolardik.

REFERENCES

1. <https://daryo.uz/>
2. <https://ictnews.uz/uz/09/07/2018/phishing>
3. <https://billur.com>
4. <https://csec.uz/uz/news/maqolalar/phishing-veb-saytlardan-ogoh-bo-ling>
5. <https://cyber-star.org/uz/cs-articles/how-to-recognize-phishing-attacks-uz>