ILM FAN XABARNOMASI
Ilmiy elektron jurnali

INTERNET FRIBGARLIK

Toshpulotov Avazbek Husan o'g'li

ANNOTATSIYA: Maqolada Internetdagi eng keng tarqalgan firibgarlik turlarining asosiy xususiyatlari (fishing, vishing, pharming, "Nigerian letters", carding) ko'rsatilgan. Shuningdek, u internet foydalanuvchilariga ushbu turdagi firibgarlikdan o'zlarini himoya qilish bo'yicha amaliy maslahatlar beradi.
Kalit so'zlar: firibgarlik turi, foydalanuvchi, Internet, to'lov kartasi, ijtimoiy muhandislik, firibgar, parol.

ANNOTATION: The article describes the main characteristics of the most common types of fraud on the Internet (Phishing, Vishing, Pharming, «Nigerian letters», Carding). In addition, it provides some practical recommendations to Internet users on how to protect themselves from this type of fraud.
Keywords: type of fraud, user, The Internet, payment card, social engineering, cheater, password.

KIRISH

O'zbekiston Respublikasining jinoyat qonunchiligida firibgarlik deganda birovning mulkini o'g'irlash yoki aldash yoki shaxsning ishonchini suiiste'mol qilish yo'li bilan birovning mulkiga bo'lgan huquqni qo'lga kiritish tushuniladi. Firibgarlik usullari har doim zamon bilan hamnafas bo'lib, dunyodagi har qanday o'zgarishlarga - yangi kommunikatsiya texnologiyalarining paydo bo'lishiga, faoliyatning yangi sohalari yoki mahsulotlarga tez moslashadi. Firibgarlar tezda o'z qurbonlarini aldash uchun ba'zan aniq va ba'zan ayyor sxemalarni ishlab chiqadilar. 1

Zamonaviy inson hayotining texnologiyalashuvi firibgarlar sonining ko'payishiga ta'sir ko'rsatdi. Internetdagi firibgarlik zamonaviy odamlarning hayotiga eng katta ta'sir ko'rsatadi, chunki Internetda odamlarni aldashning ko'plab mavjud usullari foydalanuvchilarga, ayniqsa keksa avlod vakillariga firibgarlarning hiyla-nayranglariga tayyor bo'lishga va to'g'ri munosabatda bo'lishga imkon bermaydi. Internetdagi firibgarlarning barcha sxemalari jabrlanuvchilardan to'g'ridan-to'g'ri pul yoki mulkni olishga qaratilgan emas, ko'pincha shaxsiy ma'lumotlar - loginlar, parollar, fayllarga kirish firibgarga shantaj qilish, tovlamachilik qilish yoki uni tasarruf etish imkoniyatini beradi; o'z xohishiga ko'ra ma'lumot oldi.

Onlayn firibgarlik foydalanuvchilar duch keladigan eng keng tarqalgan muammolardan biridir. Va hozirda u bilan kurashish deyarli mumkin emas, aksariyat hollarda firibgar jazosiz qolmoqda. Uning shaxsini va manzilini aniqlash juda qiyin, hatto buni amalga oshirish mumkin bo'lsa ham, uning firibgarlikka aloqadorligini isbotlash juda qiyin. U bilan kurashishning yagona samarali yo'li - aldanmaslikdir.

Shubhali tashkilotlar va xizmatlar ushbu ma'lumotlardan maqsadli reklama o'rnatish, ijtimoiy muhandislik kampaniyalarini boshlash yoki boshqa manipulyatsiya usullari orqali foydalanuvchilarga ta'sir qilish uchun foydalanadi. Bundan tashqari, moliyaviy firibgarlikning yangi usullari paydo bo'ldi. Shunday qilib, scammers, qoida tariqasida, yuqori darajadagi aql va

1 Radevich, V.V. "Nigeriya harflari" janriga asoslangan nosamimiy nutqda kommunikativ strategiya sifatida manipulyatsiyaning bosqichlari va turlari. — Matn: to'g'ridan-to'g'ri // KemDU axborotnomasi. - 2022. - No 4. - B. 121.

psixologiyani ma'lum darajada biladigan odamlardir. Ular aloqa o'rnatish va g'alaba qozonish qobiliyatiga ega. Ular, aksariyat hollarda, iqtisod, axborot texnologiyalari va boshqalar bo'yicha mutaxassislardir.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Keling, hozirgi bosqichda Internetda qanday firibgarlik turlari mavjudligini ko'rib chiqaylik:

1. “Fishing (ingliz tilidan olingan) – parollarni buzish va internetdagi maxfiy ma’lumotlarni o‘g‘irlashning eng mashhur usuli. Masalan: kredit karta to'lovi ma'lumotlari, bank foydalanuvchi nomi va paroli, foydalanuvchining shaxsiy sahifalaridagi ma'lumotlar, bank hisoblariga kirish, moliyaviy ma'lumotlar va boshqalar - har qanday ma'lumotlar firibgarlar uchun katta qiziqish uyg'otadi. Ushbu ma'lumotni olish uchun ular har xil hiyla-nayranglarga murojaat qilishadi: ommaviy elektron pochta xabarlarini (spam), davlat va moliyaviy tashkilotlardan, ijtimoiy tarmoqlardan shaxsiy xabarlarni yuborish, fishing saytlarini yaratish, sahifalar, qalqib chiquvchi oynalarni yuklash va hokazo.2

Fishingning asosiy elementi foydalanuvchi parolini yoki boshqa himoyalangan ma'lumotlarni o'g'irlash uchun ma'lum veb-saytning dublikatini yoki klonini yaratish jarayonidir. Ushbu usul juda mashhur bo'ldi, chunki ko'pchilik foydalanuvchilar kibergigienaning asosiy talablariga rioya qilmaydi. Ko'pgina hollarda, soxta sahifa va haqiqiy sahifa o'rtasidagi yagona farq uning noto'g'ri URL manzilidir (masalan, twiter.com yoki twietter.com yoki asl sahifaga o'xshash boshqa URL). Foydalanuvchilar ko'pincha sahifaning manzil satriga e'tibor bermaydilar. Va fishing sahifasining paydo bo'lishi asl sayt sahifasini to'liq nusxalashi sababli, ko'pchilik foydalanuvchilar hiyla-nayrangga tushib qolishadi va maxfiy ma'lumotlarni tajovuzkorlar bilan baham ko'rishadi.

Fishingga qanday qarshi turish kerak? begonalar tomonidan yuborilgan havolalarni bosmang; insta.gram yoki yan.dex kabi qisqa havolalarga amal qilmang, hatto bu havolalar do'stlar tomonidan yuborilgan bo'lsa ham; to‘lov va pochta tizimlarida, shuningdek, bank hisobvaraqlarida ko‘p faktorli avtorizatsiya tizimini yo‘lga qo‘yish; to'lov operatsiyalari uchun tez-tez foydalanadigan saytlar manzillarini sevimlilaringizga saqlang; allaqachon fishingdan himoyalangan brauzerlardan foydalaning (masalan, Chrome, Safari, Firefox). 3

2. “Vishing (inglizcha vishing , Voice phishing dan) ijtimoiy injeneriyadan foydalangan holda firibgarlik usullaridan biri bo‘lib, u telefon aloqasidan foydalangan holda va ma’lum rol o‘ynagan (bank xodimi, xaridor va boshqalar) firibgarlardan iborat. turli bahonalar to‘lov kartasi egasidan maxfiy ma’lumotlarni o‘ziga tortadi yoki uni karta hisobvarag‘i/to‘lov kartasi bilan muayyan harakatlar qilishga undaydi”. [5] Fishingning odatiy misoli, to'lov tizimining mijozlari ushbu tizim ma'muriyati yoki xavfsizlik xizmatidan o'z akkauntlari, parollari va boshqalarni ko'rsatishni so'rab elektron pochta xabarlarini olishlaridir. Bundan tashqari, xabardagi havola soxta saytga olib keladi. ma'lumotlar o'g'irlangan. Ushbu sayt bir muncha vaqt o'tgach yo'q qilinadi va uning

---

2 Asr talon-tarojini uyushtirgan xakerlar jinoiy javobgarlikka tortildi. — Matn: elektron // Kompyuter jinoyati tahlili va yangiliklari: [veb-sayt]. — URL: http://carderplanet.blogspot.com/2009/11/blog-post_6568.html (kirish sanasi: 12/02/2020).

3 Fishing hujumi nima va undan qanday qochish kerak? — Matn: elektron // Yandex Q: [veb-sayt]. — URL: https://yandex.ru/q/question/computers/chto_takoe_fishing_phishing_ataka_i_kak_94997200 (kirish sanasi: 30.11.2020).

yaratuvchilarini Internetda kuzatish juda qiyin. Vishing holatida aldash sxemalari bir xil. Faqat vishing holatida xabarda ma'lum bir mahalliy raqamga qo'ng'iroq qilish so'rovi mavjud. Bunday holda, potentsial jabrlanuvchidan uning maxfiy ma'lumotlarini taqdim etish so'raladigan xabar o'qiladi.

3. “ Pharming - bu qurbonni soxta IP manzilga yashirin tarzda yo'naltirish tartibi . Klassik fishingda tajovuzkor ijtimoiy tarmoqlar, onlayn-banking va veb-pochta xizmatlari foydalanuvchilariga elektron pochta xabarlarini tarqatadi va firibgarlik qurboni bo'lgan foydalanuvchilarni foydalanuvchi nomlari va parollarini olish uchun soxta saytlarga jalb qiladi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Zamonaviy veb-xizmatlardan faol foydalanadigan ko'plab foydalanuvchilar fishingning o'xshash holatlariga bir necha marta duch kelishgan va shubhali xabarlardan ehtiyot bo'lishadi. Klassik fishing sxemasida, butun sxemaning samaradorligini belgilovchi asosiy "zaif" bo'g'in - bu Fisherga ishonadimi yoki yo'qmi, foydalanuvchiga bog'liqlik. Shu bilan birga, vaqt o'tishi bilan foydalanuvchilarning fishing hujumlari haqida xabardorligi ortib bormoqda. Banklar, ijtimoiy tarmoqlar va boshqa veb-xizmatlar ijtimoiy muhandislik usullaridan foydalangan holda turli xil firibgarlik sxemalari haqida ogohlantiradilar. Bularning barchasi fishing sxemasining javob tezligini pasaytiradi - soxta saytga kirish uchun kamroq va kamroq foydalanuvchilar aldanishi mumkin.

Shu sababli, tajovuzkorlar foydalanuvchilarni "pharming" ("pharming" - "fishing" va inglizcha "fermerlik" - dehqonchilik, chorvachilik" so'zlaridan hosil bo'lgan) deb nomlangan fishing saytlariga yashirincha yo'naltirish mexanizmini o'ylab topishdi. Buzg'unchi foydalanuvchilarning kompyuterlariga maxsus zararli dasturlarni tarqatadi, ular ishga tushirilgach, so'rovlarni ko'rsatilgan saytlarga soxta saytlarga yo'naltiradi.

Farmatsevtika hujumlaridan mutlaq himoya qilish usullari mavjud emas, shuning uchun profilaktika choralarini qo'llash kerak: Litsenziyalangan virusga qarshi dasturlardan foydalanish va muntazam yangilash; Elektron pochta himoyasidan foydalanish (oldindan ko'rishni o'chirish); Noma'lum yoki shubhali oluvchilardan elektron pochta xabarlarining qo'shimchalarini ochmang yoki yuklab olmang.

“Nigeriya xatlari” (inglizcha: Advance-fee scam , so'zma-so'z “Advance to'lov firibgarligi”) firibgarlikning keng tarqalgan turi bo'lib, o'zining eng katta rivojlanishini elektron pochta (spam) orqali ommaviy yuborishlar paydo bo'lishi bilan oldi. Harflar shunday nomlangan, chunki bu turdagi firibgarlik ayniqsa Nigeriyada, hatto Internet paydo bo'lishidan oldin, bunday xatlar salyangoz pochta orqali tarqatilganda keng tarqalgan edi.

“Carding - (inglizcha carding dan) - to'lov kartasi yoki uning egasi tomonidan boshlanmagan yoki tasdiqlanmagan rekvizitlari yordamida tranzaksiya amalga oshiriladigan firibgarlik turi. To'lov kartalari ma'lumotlari odatda onlayn-do'konlarning buzilgan serverlaridan, to'lov va hisob-kitob tizimlaridan, shuningdek shaxsiy kompyuterlardan (to'g'ridan-to'g'ri yoki masofaviy kirish dasturlari, troyanlar, formalarni tortib olish funktsiyasi bo'lgan botlar orqali (kiritilgan parollar va foydalanuvchi nomlarini ushlab turish uchun foydalaniladigan josuslik dasturlari)) olinadi.

XULOSA

Tadqiqotlar shuni ko'rsatdiki, quyidagi maslahatlar foydalanuvchilarga o'zlarini ijtimoiy tarmoqlardagi firibgarlardan himoya qilishga yordam beradi: ijtimoiy tarmoqda hisob qaydnomasini ro'yxatdan o'tkazish uchun foydalaniladigan pochta qutingiz uchun asl va murakkab parolni o'ylab toping.

1. Parolingizda bosh harfingiz yoki tug'ilgan sanangizdan foydalanish tavsiya etilmaydi, chunki bu parolni buzishning eng oson usuli
2. Agar sizda katta miqdordagi pul bo'lsa, haqiqiy kredit karta yoki onlayn hamyonni ijtimoiy tarmoq hisobingizga bog'lamang.

3. Onlayn firibgarlik bilan qanday kurashish mumkinligi haqidagi savolga javob oddiy: siz mumkin bo'lgan firibgarliklar haqida bilishingiz kerak va ularga tushib qolmaslik uchun iloji boricha hushyor bo'lishingiz kerak: noma'lum odamlarga ishonmang, tasdiqlanmagan havolalarga muntazam tashrif buyurmang. kompyuteringizni viruslar uchun tekshiring, boshqa noma'lum foydalanuvchilarga pul o'tkazmang.

FOYDALANILGAN ADABIYOTLAR

1. Radevich, V.V. "Nigeriya harflari" janriga asoslangan nosamimiy nutqda kommunikativ strategiya sifatida manipulyatsiyaning bosqichlari va turlari. — Matn: to‘g‘ridan-to‘g‘ri // KemDU axborotnomasi. - 2022. - No 4. - B. 121.
2. Fishing hujumi nima va undan qanday qochish kerak? — Matn: elektron // Yandex Q: [veb-sayt]. — URL: https://yandex.ru/q/question/computers/chto_takoe_fishing_phishing_ataka_i_kak_94997200 (kirish sanasi: 30.11.2020).
3. Nigeriya harflari. — Matn: elektron // Vikipediya: [sayt]. — URL: https://ru.wikipedia.org/wiki/Social network (kirish sanasi: 2020-yil 30-noyabr).
4. Asr talon-tarojini uyushtirgan xakerlar jinoiy javobgarlikka tortildi. — Matn: elektron // Kompyuter jinoyati tahlili va yangiliklari: [veb-sayt]. — URL: http://carderplanet.blogspot.com/2009/11/blog-post_6568.html (kirish sanasi: 12/02/2020).
5. Vadim, Sviderskiy Ehtiyot bo'ling, vishing! / Sviderskiy Vadim. — Matn: elektron // Forex Magnates ruscha versiyasi: [veb-sayt]. — URL: https://ru.forexmagnates.com/ostorozhno-vishing/ (kirish sanasi: 12/01/2020).
6. Farmatsevtika. — Matn: elektron // Vikipediya: [sayt]. — URL: https://ru.wikipedia.org/wiki/ (kirish sanasi: 2020-yil 29-noyabr).