JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH
Volume 2, Issue 9, May, 2025 Online ISSN: 3030-3508
https://spaceknowladge.com

# ONLINE SAVDOLAR VAQTIDA UYUSHTIRILADIGAN FIRIBGARLIKLAR

**Abdullaeva Ozoda Safibullaevna** [1]
[1] *Namangan muhandislik-qurilish instituti pedagogika fanlari doktori (DSc), professor*
*E-mail: ozoda.safibullayevna121620@gmail.com*
**Majidov Asadbek Obidjon o'g'li** [1]
[1] *Namangan davlat universiteti magistranti*
*E-mail: asadbek.majidov@mail.ru*

**MAQOLA MALUMOTI**

**MAQOLA TARIXI:**
*Received:20.05.2025*
*Revised: 21.05.2025*
*Accepted:22.05.2025*

**KALIT SO'ZLAR:**
*The creation of the Internet has fundamentally changed the way people live. Although the creation of the Internet has brought many benefits to people in many areas, especially in the field of trade, it also has its drawbacks. In this article, we will learn about the frauds that are organized on the networks.*

**ANNOTATSIYA:**

*Internet tarmog'ini yaratilishi insonlar hayot tarzini tubdan o'zgartirib yubordi. Insonlar internetni yaratilishi juda ko'p sohalarda, hususan savdo-sotiq sohalarida koplab foyda keltirgn bo'lsa ham o'z navbatida kamchiliklari ham yo'q emas. Ushbu maqolada biz tarmoqlarda uyushtiriladigan firibgarliklar haqida o'rganiladi.*

KIRISH. Tarmoq firibgarligi bugungi raqamli iqtisodiyotda jiddiy tashvish tug‘diradi, bu jismoniy shaxslar, korxonalar va umumiy iqtisodiy manzaraga keng ko'lamli ta’sir

ko‘rsatadi. Ushbu turdagi firibgarlik keng qamrovli noqonuniy faoliyatni, jumladan, shaxsiy ma'lumotlarni o'g'irlash, fishing, to'lov dasturi hujumlari va onlayn firibgarlikning turli shakllarini o'z ichiga oladi. Tarmoq firibgarligining keng tarqalgan tabiati global iqtisodiyotning o'zaro bog'liqligi, shuningdek, moliyaviy operatsiyalarni amalga oshirish va maxfiy ma'lumotlarni saqlash uchun raqamli texnologiyalarga tobora ortib borayotgan bog'liqlikning mahsulotidir. Ushbu maqolada bir qancha tarmoq firibgarlari haqida va ulardan himoyalanish haqida o'rganimiz.

Birinchisi bu eng keng tarqalgani - fishing (phishing) hujumidir. Bunda xuddi baliq oviga o’xshash jarayon bo’ladi. Firibgar soxta saxifani xo’rak qilib tashlaydi va o’ziga kerakli ma’lumotni oladi. Phishing – bu kiberfiribgarlar tomonidan ishlatiladigan aldov usuli bo‘lib, ularning maqsadi odamlarni soxta sahifalarga yo‘naltirib, shaxsiy yoki moliyaviy ma’lumotlarini qo‘lga kiritishdir. Bu usul orqali firibgarlar foydalanuvchilarning login va parollari, bank kartasi ma’lumotlari, shaxsiy ma’lumotlari va boshqa maxfiy ma’lumotlarini o‘g‘irlashadi. Bu qanday ishlaydi? Firibgarlar sizga bank, ijtimoiy tarmoq yoki boshqa tshkilot nomidan xat yoki SMS yuborishadi. Xat yoki SMS ichida havola bo’lib, uni bosganingizda siz soxta sahifaga yo’naltirilasiz. Ushbu sahifa asl saytga juda o’xshash bo’ladi, lekin u firibgarlar tomonidan yaratilgan bo’ladi. Siz login, parol yoki karta ma’lumotlarini kiritganingizda, ular firibgarlar qo’liga tushadi. Soxta veb-sahofalardan foydalanish (Fake Websites) Firibgarlar asl saytga o’xshash soxta sayt yaratishadi. Masalan, haqiqiy sayt “ www.paypal.com “ bo’lsa, soxta saxifa “ www.paypall.com ”, yoki “ www.pay-pal.com ” kabi o’xshash nomad bo’lishi mumkin. Foydalnuvchi e’tibor bermay, parol yoki boshqa ma’lumotlarini kiritib yuborishi mumkin. Yana bir usul ijtimoiy tarmoqlar orqali phishing. Firibgarlar Facebook, Instagram, Telegram kabi ijtimoiy tarmoqlarda mashhur shaxs yoki kompaniya sifatida soxta akkaunt ochishadi. Shundan so’ng ular foydalanuvchilarga yutuq, aksiya yoki boshqa narsa bahona qilib, maxsus sahifaga kirishni taklif qilishadi. Ushbu sahifada foydalanuvchi login va parolini kiritganidan keyin, uning akkaunti friribgarlar qo’liga tushadi. Firibgarlar telefon orqali ham phishing hujum qilishadi (Vishing-voice Phishing) bu qanday ishlaydi keeling shu haqida gaplashaylik. Firibgarlar telefon orqali bank yoki boshqa tashkilot vakili sifatida qo’ng’iroq qilib, shaxsiy ma’lumotlarni so’rashadi. Ular hisobingiz buzilganini yoki pul o’tkazishingiz kerakligini aytib, ma’lumotlaringizni olishga harakat qilishadi. Bu usul orqali hujumlar ayniqsa hozirgi kunda ko’paymoqda. Ba’zan phishing sahifalarida keylogger yoki boshqa zararli dasturlar joylashtiriladi. Agar foydalanuvchi ushbu sahifaga kirsa yoki zararli faylni yuklab olsa, uning kompyuteridagi harakatlar kuzatiladi va parollar o’g’irlanadi. Smashing

nomli hujum turi ham mavjud bo'lib, bu ham phishingga o'xshaydi, lekin electron pochta xabari o'rniga SMS xabar ishlatiladi. Foydalanuvchi raqamga qo'ng'iroq qilish yoki havolani bosish so'ralgan SMS xabar yuboriladi. Ushbu raqamga telefon qilinganda qo'ng'iroqni qabul qilgan kishi qo'ng'iroq qiluvchidan shaxsiy ma'lumotlarni olishga harakat qiladi. Shuningdek, qo'ng'iroq qiluvchidan qo'ng'iroq uchun katta miqdorda pul olinishi mumkin. Havola bosilganda zararli daatur foydalanuvchining telefoniga yuklab olinadi. Zararli dastur foydalanuvchi ma'lumotlarini to'plash, shaxsga nisbatan tovlamachilik qilish va o'g'irlik uchun ishlatiladi. U qurilmani bot tarmog'ining bir qismiga ham aylantirishi mumkin. Keyingi bosqichda ushbu qurilma xizmatni rad etish hujumlari uchun ishlatilishi mumkin. Havola foydalanuvchini phishingda bo'lgani kabi, qonuniy ko'rinadigan veb saytga olib borishi va foydalanuvchining shaxsiy ma'lumotlari o'zlashtirilishiga olib kelishi ehtimoli ham bor. Smishing ko'pincha foydalanuvchini raqamga qo'ng'iroq qilishga yoki havolani bosishga undaydi, agar shunday qilinsa, tovlamachilar olishlari mumkin bo'lgan daromad haqida, masalan, mahsulot va xizmatlarga chegirma taqdim etuvchi vaucher yoki sovg'a kartasi borasida maslahat berishadi. Smishingdan foydalanish tobora ortib bormoqda. Buning sababi odamlarning kompyuterlarga yuborilgan xabarlarga nisbatan telefonlariga jo'natilganiga kamroq shubha bilan qarashlaridir. Aksariyat yirik veb brauzerlarining phishingga qarshi himoyasi bor, bu foydalanuvchini ehtimoliy phishing xatari to'g'risida ogohlantirishga yordam beradi. Mobil telefonlar esa bunday jhozlanmagan.

Smishingdan himoyalanish uchun bajarilishi kerak bo'lgan choralar:

- Foydalanuvchilar SMS xabar orqali yuborilgan raqamlarga telefon qilishda juda ehtiyot bo'lishlari kerak.
- Foydalanuvchilar xabarlardagi har qanday havolani bosishda juda ehtiyot bo'lishlari kerak.
- Foydalanuvchilar o'zlari bilmagan yuboruvchilarning biron-bir dasturini o'rnatmasligi kerak.
- Agar foydalanuvchi tanigan kishisidan shubhali xabar oladigan bo'lsa, ushbu xabarni haqiqatan ham u yozganini tekshirish kerak.
- Foydalanuvchilar odatdagi mobil raqamlarga o'xshamaydigan raqamlardan, masalan, "5000" dan ehtiyot bo'lishlari kerak.
- Foydalanuvchilar har qanday zararli dasturni aniqlashga yordam berishi uchun mobil telefonlariga xavfsizlik dasturlarini qo'shishlari mumkin.


Korzinka.uz'dan ekanini da'vo qiladigan smishing xabariga misol.

Vishing hujumlari haqida ham gapirmasak bo'lmaydi. Vishing – ovozli phishingning qisqa shakli. Bu foydalanuvchidan shaxsiy ma'lumotlarni olishi uchun qo'ng'iroq qilib, ularni undash yoki aldash amaliyoti. Firibgar odatda birovga vakili ekanini uqtirmoqchi bo'ladi. Vishing bilan shug'ullanayotgan odam shaxsning akkaunti bilan bog'liq muammo haqida jabrlanuvchini ogohlantirishi yoki unga foydali daromad haqida taklif bildirishi mumkin. Ular ko'pincha kerakli shaxsiy ma'lumotlarni olish uchun jabrlanuvchiga nozik savollar berishadi. Ba'zan malakali vishingchilar jabrlanuvchilar biroz shubhalanib qolsa va qo'ng'iroq qonuniyligini tekshirish uchun o'z bankiga qo'ng'iroq qilmoqchi bo'lsa, telefonni qo'yib qo'ymaydi. Keyin esa jabrlanuvchi o'z bankiga qo'ng'iroq qilish uchun telefonni oladi, ammo bu tarmoq hanuzgacha firibgar tomonidan ushlab turilgan bo'ladi. Jabrlanuvchi o'z bankimga qo'ng'iroq qildim, deb o'ylaydi, ammo bu hali ham firibgar bo'lib, jabrlanuvchi unga shaxsiy ma'lumotlarini taqdim etadi. Afsuski, ko'pincha qariyalar va zaif odamlar vishing qurboniga aylanishadi. Vishingdan himoyalanish uchun bajarilishi kerak bolgan choralar:

- Odamlar har qanday muassasa ular bilan bog'langanida, ayniqsa, shaxsiy ma'lumotlar so'ralganda, ehtiyot bo'lishlari kerak. Agar shubhalasangiz, telefonni o'chirib qo'ying va mavjud raqamga qayta qo'ng'iroq qiling.
- Odamlar hech qachon o'zlarining akkauntlari xavfsizligi bilan bog'liq shaxsiy ma'lumotlarni hech kimga bermasliklari kerak. Banklar akkauntga qaratilgan har qanday hujumdan akkaunt egasidan yordam olmay himoyalana oladi.

Zararli dastur-kompyuter tizimiga va unda saqlanadigan fayllarga zarar yetkazish yoki buzish uchun mo'ljallangan kompyuter dasturi. Zararli dastur turli shakllarda bo'lishi mumkin va biz ularning bir nechtasini ko'rib chiqamiz.

Troya oti (troyan) – zararli kompyuter dasturi bo'lib, o'zini boshqa dastur, masalan, o'yin yoki yordamchi dastur sifatida yashiradi. Dastur ishga tushirilgach, Troya oti kompyuter

virusi kabi harakat qila boshlaydi, kompyuter tizimidagi fayllarni yo'q qiladi va buzadi. "Troya oti" atamasi yunon mifologiyasiga borib taqaladi. Troya shahri aholisiga tinchlik sulhi sifatida yog'och ot beriladi. Troya oti aslida bir qancha yunon askarlari ichiga kirib olgan moslama edi. Askarlar qorong'i tushganda ot ichidan chiqib, Shahar darvozasini ochib beradi. Bu payt tashqarida Troya shahrini zabt etishga qodir qo'shin payt poylab turgan bo'ladi. Zararli Troya oti dasturi xuddi shunday ishlaydi. Yaxshi dasturlar kabi ko'rinadi, ammo uning ichida zararli dastur yashiringan bo'ladi.

Kompyuter qurti – kompyuter tarmoqlaridan foydalanadigan va o'zini ishga tushurish uchun xavfsizlik teshiklarini topadigan kichik kompyuter dasturlaridir. Ular dasturiy ta'minot yoki operatsion tizimdagi xavfsizlik nuqsonlaridan foydalanishi mumkin. O'zini ishga tushirish paytida ular ko'pincha tarmoqning o'tkazuvchanligini to'sib qo'yadi va ish jarayonini sekinlashtiradi. Bir nechta mashhur kompyuter qurtlari bor. Ulardan biri Code Red ("Qizil kod") deb nomlanadi. Code Red 2001-yilda paydo bo'lgan va bir necha soat Ichida o'zini 250000 martadan ortiq ishga tushirishga – replikatsiya qilishga erishgan. U Windows serverlarini toppish uchun internetni skanerdan o'tkazgan. Bunda Microsoftning xavfsizlik tuzatishlarini o'rnatmagan qurilmalarining xavfsizlik teshiklari, ya'ni nuqsonlaridan foydalangan.u har safar zaif serverni topganda, o'zini serverda ishga tushirgan va keyingisini toppish uchun harakatda davom etgan. Keyin esa barcha zararlangan serverlar Oq uyning www.whitehouse.gov domeniga hujum qilishni boshlagan.

Josus dasturlar zararli dasturlarning juda keng doirasini qamrab oladi. Bu atama inson haqida unga bildirmasdan ma'lumot to'plash uchun ishlatiladigan har qanday texnalogiyani anglatadi. Dastur ko'pincha odamlarning harakatini onlayn tarmoq orqali kuzatib borish uchun ishlatiladi. Sopyware dasturlarining keng tarqalgan turo klaviatura josusi hisoblanadi. Bu klaviaturada bosilgan tugmalarni yozib oladigan va uni o'rnatgan odamga shaxsiy ma'lumotlarni to'plash imkonini beradigan dasturiy ta'minot.

Zararli dasturlardan saqlanish uchun ushbu qoidalarga amal qiling:

- Dasturning qonuniyligiga ishonchingiz komil bo'lmasa, uni hech qachon ochmang.
- Internet tafigini kuzatadigan fayervol o'rnating.
- Zararli dastur mavjudligini aniqlash uchun muntazam ravishda kompyuter tizimida antivirus tekshiruvi va zararli dasturlarni aniqlash dasturini yoki zararli dasturlarni aniqlash dasturini yangilab turing. Shundagina u yangi chiqqan zararli dasturlarni aniqlay oladi.
- Noma'lum foydalanuvchilarning elektron pochta xabarlaridagi hech qaysi biriktirilgan faylni ochmang.

- Ochiq Wi-Fi nuqtalaridan juda ehtiyotkorlik bilan foydalaning, chunki ularga hamma ulanishi mumkin.

Har qanday turdagi firibgarlik ham sizning ma’lumotlaringiz va pullaringizga ziyon keltirishi mumkin. Biz yuqorida bir nechta firibgarlik usullarini ko’rdik va ularga yechim berishga harakat qildik. Aslida kundan kunga firibgarlar yangidan yangi usullarni qo’llashmoqda. Har qanday holatta ham foydalanuvchilardan ehtiyotkorlik va har qanday ma’lumotni asosli yoki asossizligini tekshirishni so’rab qolamiz.

## Foydalangan adabiyotlar:

1. Safibullaevna, A. O., Engalichev, M. I., & Safibullaevna, B. S. (2020, November). Online-learning organization methodology as component of it technologies at students of technical universities. In *2020 International Conference on Information Science and Communications Technologies (ICISCT)* (pp. 1-6). IEEE.
2. Safibullayevna, A. O. (2023). Intelektual axborot bilimlar tizimini xususiyatlari, belgilari va imkoniyatlari. *IJODKOR O'QITUVCHI*, *3*(28), 121-126.
3. Abdullayeva, O. S., & Muhammadjonov, A. O. (2023, September). Modeling the Development of Department Activities in Higher Education Institutions: Enhancing the Management System with Quantum Communication and Cryptography%. In *2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET)* (pp. 588-591). IEEE.
4. Safibullaevna, A. O., & Azamxonov, B. S. (2024). TECHNOLOGY OF CREATION AND APPLICATION OF AN INTELLIGENT INFORMATION SYSTEM. *CURRENT RESEARCH JOURNAL OF PEDAGOGICS*, *5*(01), 31-38.
5. Ozoda, A., & Azamxonov, B. S. (2023). MEANS OF ORGANIZING AN INTELLIGENT INFORMATION SYSTEM. *Innovations in Technology and Science Education*, *2*(17), 438-449.
6. Safibullaevna, A. O. (2022). Foreign experience in the preparation of master's programs aimed at the development of information and management competences. *Current research journal of pedagogics*, *3*(03), 41-47.
7. Абдуллаева, О. С. (2015). Анализ учебно-воспитательной деятельности учащихся в процессе изучения дисциплины" Информатика и информационные технологии". *Молодой ученый*, (12), 687-690.

8. Абдуллаева, О. С. (2016). Формирование и развитие педагогических способностей в процессе непрерывного образования. *Евразийский союз ученых*, (3-2 (24)), 91-92.

9. Абдуллаева, О. С. (2014). Современное состояние подготовки будущих учителей информатики к педагогической деятельности. *Современное образование (Узбекистан)*, (10), 34-39.

10. Абдуллаева, О. С. (2016). Измерительный инструмент (индикаторы) для определения готовности студентов ВУЗа к педагогической деятельности. *Современное образование (Узбекистан)*, (6), 26-33.

11. Абдуллаева, О. С. (2015). Формирование умений и навыков у учащихся средних специальных профессиональных образовательных учреждений. *Дистанционное и виртуальное обучение*, (3), 99-106.

12. АБДУЛЛАЕВА, О. (2024). ЦИФРОВЫЕ МЕТОДЫ СОЗДАНИИ ДИНАМИЧЕСКОГО САЙТА ДЛЯ ВОУ. *News of the NUUz*, *1*(1.9. 1), 63-67.

13. Abdullayeva, O., & Shermatova, M. (2024). THE SOCIO-PEDAGOGICAL NECESSITY OF IMPROVING THE SUGGESTIVE ABILITIES OF FUTURE TEACHERS OF PEDAGOGICAL SCIENCE. *Science and innovation*, *3*(B10), 52-56.

14. Safibullayevna, A. O. (2024). The Importance Of The Use Of Trainings, Methods, And Tools In The Training Of Future Preschool Educational Organizations In The Use Of Pedagogical-Psychological Characteristics Of Training Teachers. *American Journal of Advanced Scientific Research*, *1*(8), 69-71.