ONLAYN TO‘LOVLAR BILAN FOYDALANISHDAGI XATARLAR

[1] *Mamasoliyev Asilbek,Abdullayev Shaxriyor*
O‘zbekiston
[1] *Farg‘ona davlat texnika universiteti, kompyuter injenering*
IT – servis yo‘nalishi talabasi asilbekmi80@gmail.com

Annotatsiya. Ushbu maqolada onlayn to‘lov tizimlaridan foydalanish jarayonida uchrashi mumkin bo‘lgan xavf va xatarlar tahlil qilinadi. Elektron tijoratning kengayishi, raqamli bank xizmatlarining ommalashuvi va onlayn to‘lov platformalariga talab oshgani sayin, ularga nisbatan kiberjinoyatchilik darajasi ham ko‘tarilmoqda. Maqolada phishing, malware, man-in-the-middle, identifikatsiya xatolari, tranzaksiyani soxtalashtirish, ijtimoiy muhandislik hamda foydalanuvchi xatolari kabi keng tarqalgan xavflar yoritiladi. Shuningdek, xavfsizlikni ta’minlash bo‘yicha texnik va tashkiliy yechimlar taklif etiladi.

Kalit so‘zlar: Onlayn to‘lov, elektron tijorat, kiberxavfsizlik, phishing, firibgarlik, raqamli bank xizmatlari, shifrlash, autentifikatsiya, tranzaksiya xavfsizligi.

Аннотация. В данной статье анализируются риски и угрозы, которые могут возникнуть при использовании онлайн-платёжных систем. По мере расширения электронной коммерции, роста популярности цифровых банковских услуг и увеличения спроса на онлайн-платёжные платформы, уровень киберпреступности, направленной против них, также возрастает. В статье рассматриваются распространённые угрозы, такие как фишинг, вредоносное ПО, атаки типа «man-in-the-middle», ошибки идентификации, подделка транзакций, социальная инженерия, а также ошибки пользователей. Кроме того, предлагаются технические и организационные решения для обеспечения безопасности.

Ключевое слово:Онлайн-платёж, электронная коммерция, кибербезопасность, фишинг , мошенничество, цифровые банковские услуги, шифрование, аутентификация, безопасность транзакций.

Abstract. This article analyzes the risks and threats that may arise when using online payment systems. As electronic commerce expands, digital banking services become more widespread, and the demand for online payment platforms increases, the level of cybercrime targeting these systems is also rising. The article highlights common threats such as phishing, malware, man-in-the-middle attacks, identification errors, transaction forgery, social engineering, and user mistakes. In addition, it proposes technical and organizational measures to ensure security.

Keyword Online payment, electronic commerce (e-commerce), cybersecurity, phishing, fraud, digital banking services, encryption, authentication, transaction security.

Kirish. So‘nggi yillarda dunyo raqamli iqtisodiyot tomon jadal harakat qilmoqda. Naqd pulsiz iqtisodiyotning shakllanishi jarayonida elektron to‘lov tizimlari, mobil banking, onlayn savdo maydonchalari, QR-kod to‘lovlari, virtual kartalar, hamda elektron hamyonlar keng tarqaldi. Ushbu xizmatlar odamlarning kundalik hayotida muhim o‘rin egallab, qulaylik yaratmoqda: tezkor to‘lov, 24/7 faoliyat, geografik cheklovlarning yo‘qligi, xizmatlar diversifikatsiyasi va boshqalar. Biroq, onlayn to‘lovlar kengaygani sari, ularning xavfsizligiga bo‘lgan ehtiyoj ham kuchaydi. Bugungi kunda kiberjinoyatchilar nafaqat murakkab texnik vositalardan, balki psixologik manipulyatsiyalardan ham foydalanmoqdalar. Global statistika ko‘rsatkichlariga ko‘ra, har yili milliardlab dollarlar miqdorida zarar onlayn to‘lov firibgarliklari tufayli yuzaga kelmoqda. Bu jarayonning tez sur’atlarda o‘sishi, xatarlar spektrining kengayishi va ilg‘or texnologiyalar qo‘llanishi muammoni yanada keskinlashtirib bormoqda. Onlayn to‘lovlar bilan bog‘liq xatarlar nafaqat

foydalanuvchilarga, balki banklarga, servis provayderlarga, elektron tijorat subyektlariga ham xavf tug‘diradi. Shu sababli mazkur mavzuni chuqur o‘rganish elektron to‘lov tizimlari xavfsizligini ta’minlashda muhim ahamiyatga ega. 1. Onlayn to‘lov tizimlari va ularning ahamiyati: Onlayn to‘lov tizimlari bank kartalari, elektron hamyonlar, mobil to‘lovlar, internet-banking, QR-kod to‘lovlari, NFC (Near Field Communication) to‘lovlari kabi turli texnologiyalarni o‘z ichiga oladi. Elektron to‘lovlar iqtisodiyotning quyidagi jihatlariga sezilarli ta’sir ko‘rsatadi: 1.1. Tezkorlik va qulaylik: Tranzaksiyalar bir necha soniyada amalga oshadi. An’anaviy bank jarayonlarida esa bu bir necha daqiqadan bir necha soatgacha davom etardi. 1.2. Xarajatlarning kamayishi: Naqd pul aylanishini qisqartirish orqali banklar, korxonalar va davlat tizimi xarajatlarini pasaytiradi. 1.3. Raqamli iqtisodiyotni rivojlantirish: Onlayn to‘lov infratuzilmasi elektron tijorat, FinTech xizmatlari, avtomatlashtirilgan to‘lov tizimlari rivojlanishiga xizmat qiladi. 1.4. Moliyaviy inklyuziya: Aholining bank xizmatlariga kirish imkoniyatini kengaytiradi. Shunga qaramay, bu tizimlarning rivojlanishi bilan birga xavfsizlikka doir yangi muammolar ham yuzaga chiqmoqda. 2. Onlayn to‘lov tizimlaridagi asosiy xatarlar. 2.1. Phishing (soxta sahifalar orqali ma’lumot o‘g‘irlash) Phishing — foydalanuvchini aldash orqali uning karta ma’lumotlari, parollari yoki kodlarini qo‘lga kiritish usulidir. Jinoyatchilar bank saytiga o‘xshash soxta sahifa yaratib, foydalanuvchini unga o‘tishga majbur qiladi. Eng keng tarqalgan phishing usullari: Soxta SMS xabarlar. Bank nomidan yuborilgan elektron pochta, messengerdagi yolg‘on havolalar, soxta mobil ilovalar Ko‘pincha xabar matnida “Kartangiz bloklandi”, “Shaxsiy kabinetga kiring”, “To‘lovni tasdiqlang” kabi shoshilinch mazmun bo‘ladi. 2.2. Malware (zararli dasturlar) Zararli dasturlar foydalanuvchining qurilmasiga yashirincha o‘rnashib, uning to‘lov ma’lumotlarini o‘g‘irlaydi. Mashhur malware turlari: Keylogger — klaviaturada bosilgan tugmalarni yozib boradi; Trojan — bank ilovalari ko‘rinishida o‘rnatiladi; Spyware — foydalanuvchi ekranini kuzatadi; Ransomware — to‘lov talab qilib ma’lumotlarni bloklaydi. Bank ilovalariga soxta versiyalarning tarqalishi bugungi kunda eng faol ko‘rinishlardan biridir.

2.3. Man-in-the-Middle (MITM) hujumlari. Bu hujum turi foydalanuvchi va server o‘rtasidagi aloqaga aralashish orqali amalga oshiriladi. Jinoyatchi tranzaksiyani kuzatadi, o‘zgartiradi yoki to‘lovni boshqa hisob raqamiga yo‘naltiradi. MITM ko‘pincha:

himoyalanmagan Wi-Fi tarmoqlarida, g‘ayriqonuniy Wi-Fi nuqtalarida, noto‘g‘ri SSL sertifikatlarida uchraydi.

2.4. Identifikatsiya va autentifikatsiya xatolari;

Foydalanuvchining shaxsini aniqlashda kamchilik bo‘lsa, hisobga noqonuniy kirish sodir bo‘lishi mumkin. Keng tarqalgan muammolar:

- Zaif parol tanlash;
- Bitta paroldan ko‘p joyda foydalanish;
- Ikki bosqichli (2FA) himoya o‘chirilgan bo‘lishi;
- SMS-kodlarni uchinchi shaxsga berish.

Bugungi kunda ijtimoiy tarmoqlarda “verifikatsiya xizmatlari” niqobi ostida odamlarni aldash holatlari ko‘p.

2.5. Tranzaksiyani soxtalashtirish

- Kiberjinoyatchilar quyidagi yo‘llar yordamida tranzaksiyani o‘zgartirishi mumkin:
- Rekvizitlarni almashtirish;
- To‘lov miqdorini oshirish;
- Qayta yo‘naltirilgan tranzaksiyalar;
- “Double spending” usullari.

Elektron to‘lov tizimlari blokcheyn kabi texnologiyalar bilan mustahkamlangan bo‘lsa-da, ba’zi an’anaviy tizimlarda bunday muammolar uchraydi.

2.6. Ijtimoiy muhandislik (social engineering)

Jinoyatchilar texnik vositadan ko‘ra, inson psixologiyasidan foydalanadi:

Bank xodimi sifatida qo‘ng‘iroq qilish

“Kartangiz bloklandi” deb qo‘rqitish

“Bonus yutdingiz” orqali aldash

Qarindosh nomidan yozish

Telegram/WhatsApp orqali “kodni yuboring” deb aytish

Bu ko‘pincha eng samarali hujum turidir, chunki foydalanuvchining o‘zi ma’lumotni topshiradi.

2.7. Foydalanuvchi xatolari:

Onlayn to‘lov xavflarining 40% dan ortig‘i foydalanuvchining bexato harakat qilolmasligi bilan bog‘liq:

- Karta ma’lumotlarini tanishlarga yuborish
- To‘lovni tasdiqlashdan oldin tekshirmaslik
- Soxta saytni asl saytdan ajrata olmaslik
- Noto‘g‘ri rekvizit kiritish
- Shubhali ilovalarni o‘rnatish
- Odatda firibgarlik “oddiy xatolik” orqali boshlanadi.

3. Onlayn to‘lovlar xavfsizligini ta’minlash usullari;

3.1. Texnik himoya choralari;

3.1.1. Shifrlash (Encryption)

HTTPS, SSL/TLS protokollari ma’lumotlarni uchinchi shaxs ko‘rmasligi uchun shifrlaydi.

3.1.2. Tokenizatsiya

Karta raqami o‘rniga token ishlatiladi. Token o‘g‘irlangan taqdirda ham foydasiz.

3.1.3. 3D-Secure (Verified by Visa, MasterCard SecureCode)

Tranzaksiyani qo‘shimcha tasdiqlash talab qilinadi.

3.1.4. Firewall va IDS/IPS tizimlari

Serverlarga noqonuniy trafikni bloklaydi.

3.2. Tashkiliy va boshqaruv tadbirlari

- Muntazam kiberxavfsizlik auditi
- Bank tizimida xodimlarga trening

•Katta summali tranzaksiyalar uchun qo‘shimcha verifikatsiya

•Zaxira nusxalar yaratish

•Kiberjinoyatchilik bo‘yicha qonunchilikni kuchaytirish

3.3. Foydalanuvchi xavfsizligi bo‘yicha tavsiyalar:

•Hech qachon bank kodlarini uchinchi shaxsga bermaslik

•Soxta SMS va havolalarga ishonmaslik

•Telefon orqali parol aytmaslik

•Faqat rasmiy ilovalarni o‘rnatish

•Katta summali to‘lovlarda ehtiyotkorlik

•Karta orqa tomonidagi CVV/CVC kodni hech kimga yubormaslik

4. Onlayn to‘lovlarda firibgarlik misollari:

Quyidagi real hayotdagi misollar xatarlarning qanchalik kengligini ko‘rsatadi:

4.1. Soxta “bank xodimi” qo‘ng‘iroqlari

•Jinoyatchi o‘zini bank xodimi sifatida tanishtiradi va:

•“Hisobingizda shubhali operatsiya aniqlandi. Kartangizni himoyalash uchun SMS kodni ayting”, — deb aytadi.

•Kod berilgach, pul o‘g‘irlanadi.

4.2. Onlayn savdo maydonchasidagi firibgarlik

Sotuvchi yoki xaridor sifatida aldab, “karta orqali pul o‘tkazish uchun havola yuboramiz” deb soxta to‘lov sahifasiga olib borish hollari.

4.3. Shubhali bonuslar va aksiyalar “100 000 so‘m bonus yutdingiz” tarzidagi xabarlar orqali bank ma’lumotlarini olish.

Xulosa. Onlayn to‘lov tizimlarining rivojlanishi iqtisodiy o‘sish, qulaylik, tezkorlik va raqamli xizmatlar tarmog‘ining kengayishiga katta hissa qo‘shmoqda. Biroq bu jarayon bilan birga, kiberjinoyatchilik faoliyati ham ortib bormoqda. Phishing, malware, ijtimoiy muhandislik, MITM hujumlari, tranzaksiyani soxtalashtirish kabi xavflar har yili millionlab foydalanuvchilarning moliyaviy xavfsizligiga zarar yetkazmoqda. Ushbu xavflarni kamaytirish uchun texnik (shifrlash,

tokenizatsiya, 3D-Secure), tashkiliy (audit, treninglar) va foydalanuvchi (ehtiyotkorlik, ma’lumotlarni sir saqlash) darajasida kompleks chora-tadbirlar amalga oshirilishi zarur. Xulosa qilib aytganda, onlayn to‘lovlardan xavfsiz foydalanish texnologiya, menejment va foydalanuvchi madaniyatining uyg‘unlashgan holda olib borilishiga bog‘liqdir.

Foydalanilgan adabyotlar

Kaspersky Cybersecurity Blog

Mavzular: phishing, malware, MITM hujumlari, onlayn to‘lov xavfsizligi.

Manba: Kaspersky Security Articles – https://www.kaspersky.com/blog/

OWASP (Open Web Application Security Project)

Mavzular: web xavfsizlik, autentifikatsiya xatolari, MITM, zaifliklar.

Manba: OWASP Top 10 – https://owasp.org/www-project-top-ten/

Statista – Online Payment Fraud Reports

Mavzular: global firibgarlik statistikasi, raqamli to‘lovlar bo‘yicha statistik ma’lumotlar.

Manba: Statista Digital Payments Security – https://www.statista.com/

NIST (National Institute of Standards and Technology)

Mavzular: shifrlash, autentifikatsiya, kiberxavfsizlik bo‘yicha standartlar.

Manba: NIST Cybersecurity Framework – https://www.nist.gov/cyberframework

Schneier on Security (Bruce Schneier blogi)

Mavzular: kiberjinoyatlar, social engineering, to‘lov tizimlaridagi xatarlar.

Manba: https://www.schneier.com/