ONLAYN INTERNET DO‘KONLARNING XAVFSIZLIGINI TA’MINLASH USULLARI

TO‘YCHIYEV XURSHIDBEK MUXAMATVALI O‘G‘LI
O‘zbekiston xalqaro islom akademiyasi
“Zamonaviy axborot-kommunikatsiya
texnologiyalari” kafedrasi o‘qituvchisi

Anotatsiya.*Ushbu maqolada web saytlar va onlayn internet portallarining axborot xavfsizligiga bo‘ladigan tahdidlar va hujumlarni o‘rganish, hamda ularning axborot xavfsizligini ta’minlash usullari tahlil qilingan.*

Kalit so‘zlar: *Kredit karta firibgarligi, parol buzish, zararli dasturiy ta’minot va veb-ilovalar hujumlari, fishing, front-end, back-end.*

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНТЕРНЕТ-МАГАЗИНОВ

Аннотация.*В данной статье рассматриваются угрозы и атаки на информационную безопасность веб-сайтов и интернет-порталов, а также анализируются способы обеспечения их информационной безопасности.*

Ключевые слова: *мошенничество с кредитными картами, взлом паролей, атаки вредоносных программ и веб-приложений, фишинг, front-end, back-end.*

METHODS OF ENSURING SECURITY OF ONLINE INTERNET STORES

Abctract.*This article analyzes the study of threats and attacks on information security of websites and online internet portals, as well as ways to ensure their information security.*

Keywords: *credit card fraud, password hacking, malware and web app attacks, phishing, front-end, back-end.*

Kirish.

Raqamli dunyo potentsial xaridorlarni qanday tovar yoki xizmatlarga qiziqtirishidan qat'iy nazar ularni qul qilishda davom etmoqda. So‘nggi tadqiqotlar shuni ko‘rsatdiki, ko‘pchilik iste'molchilar mahsulot sotib olishdan oldin u haqida ma'lumotni Internetdan mahsulotni sotadigan saytlardan izlaydilar. Ba'zilar buni shunchaki do‘konga borib, o‘zlari qilish uchun vaqtlari yoki imkonlari yo‘qligi uchun qilsa, boshqalari buni tezroq va qulayroq bo‘lgani uchun qilishadi. Ularning motivlaridan qat'iy nazar, natijada mijozlar bilan asosiy ish asta-sekin raqamli makonga o‘tadi.

Bunday jadal rivojlanayotgan tendentsiya fonida veb-sayt yoki onlayn internet portalini yaratish va bu orqali insonlarga foyda ulashish, jamiyatimiz aholisini rivojlantirish uchun juda ajoyib g'oyadir. Onlayn portal yaratish saytning eng samarali tashkil etilishi, uni raqamli dunyoda targ'ib qilish usullari va boshqa ko‘plab muhim bilimlarni talab qiladi. Bularning barchasi birgalikda sizga foyda keltiradigan yuqori sifatli internet mahsulotini yaratish uchun juda muhimdir.

Masalaning qo‘yilishi. Onlayn veb portal yaratar ekanmiz xavfsizligini ham unutmasligimiz lozim. Foydalanuvchilarning shaxsiy ma'lumotlarining maxfiyligiga, shuningdek, to‘lov usullarining xavfsizligiga e'tibor berish kerak. Bu sizning onlayn do‘koningizga ishonchni oshirishga yordam beradi.

Onlayn internet portalida axborot xavfsizligini ta'minlash uchun eng avvalo axborot xavfsizligiga bo‘ladigan tahdidlar va hujumlar bilan tanishib chiqishimiz lozim. Bugungi kunda eng keng tarqalgan zamonaviy tahdid va kiberhujumlarga quyidagilar kiradi:

- kredit karta firibgarligi
- parolni buzish
- zararli dasturiy ta'minot va veb-ilovalar hujumlari
- spam yuborish
- fishing

Kredit karta firibgarligi bu onlayn do‘kon duch kelishi mumkin bo‘lgan eng yomon muammolardan biridir. Sizning veb-saytingizda saqlanadigan ma’lumotlar o‘g'irlanishi va naqd pul olish yoki ruxsatsiz xaridlarni amalga oshirish uchun ishlatilishi mumkin. Kredit karta ma’lumotlari onlayn-do‘kon egalari va do‘kon xaridorlari uchun xavf tug'diradi. Bundan tashqari, u brendning obro‘sini buzadi va bankrotlikka olib kelishi mumkin.

Parolni buzish. Veb-sayt ma’lumotlar bazasida saqlanadigan shaxsiy va moliyaviy ma’lumotlar nozik ma’lumotlar hisoblanib, parolni buzib o‘tish bilan o‘g‘irlanishi mumkin. Parol buzib o‘tilgandan so‘ng biror narsa sodir bo‘lganda birinchi bo‘lib onlayn kitob do‘koni egasi aybdor bo‘lmasliklari uchun bu asosiy masalalardan biri hisoblanadi va bu masalaga chora ko‘rish kerak.

Zararli dasturlar va veb-ilovalar hujumlari. Zararli dasturlar, josuslik dasturlari, viruslar va to‘lov dasturlari raqamli qurilmalarga o‘rnatilishi, veb-serverni buzishi va maxfiy ma’lumotlarni o‘g'irlashi mumkin. Zararli dasturiy ta’minot bilan birgalikda veb-ilova hujumlari onlayn do‘konlarga jiddiy tahdid soladi. Noto‘g'ri kodlangan ilovalar juda ko‘p zaif tomonlarga ega, bu esa ma’lumotlar bazalarini buzishni hech qanday muammosiz amalga oshia oladi.

Spam yuborish. Spam - bu sizning veb-saytingizda mavjud bo‘lgan elektron pochta, ijtimoiy tarmoqlar, sharhlar va aloqa shakllari orqali infektsiyalangan havolalarni yuborish va tarqatishdir. Ushbu turdagi havolalar sizni va sizning mijozlaringizni ma’lumotlar xavfsizligiga salbiy ta’sir ko‘rsatishi mumkin bo‘lgan veb-saytlarga yo‘naltiradi.

Spam yuborish onlayn do‘konlar veb-saytlari uchun jiddiy muammodir, chunki u:

– yuklanish tezligini sezilarli darajada kamaytiradi;

– veb-saytingiz ish faoliyatini yomonlashtiradi;

– veb-saytning umumiy xavfsizligini pasaytiradi.

Fishing - bu firibgarlikning bir turi, uning maqsadi foydalanuvchining maxfiy ma’lumotlari - login va parollarga kirishdir. Fishing hakerlar tomonidan nozik ma’lumotlarni olish uchun ishlatiladigan eng samarali taktika. Onlayn

xaridor noaniq manbalardan kelgan elektron pochta xabarlarini ochmasligi kerak. Bundan tashqari, agar bank onlayn xaridordan biron-bir ma’lumot talab qilsa, taqdim etishdan avval qo‘ng'iroq qilish oqilona bo‘ladi.

Ko‘pincha, kiberjinoyatchilar taniqli brendlar nomidan ommaviy elektron pochta xabarlarini, shuningdek, turli xil xizmatlar ichidagi shaxsiy xabarlarni, masalan, banklar nomidan yoki ijtimoiy tarmoqlardan yuborish orqali qimmatli ma’lumotlarni olishning oddiy, ammo samarali usullaridan foydalanadilar. Odatda, jinoyatchilar elektron pochta xabarlarini o‘lja sifatida ishlatishadi. Shu bilan birga, bunday bildirishnomalar odatda "rasmiy" ko‘rinishga ega bo‘lib, natijada foydalanuvchi ularni jiddiy qabul qiladi. Bunday xatlardan odam turli bahonalar bilan ko‘rsatilgan saytga kirib, so‘ng avtorizatsiya uchun foydalanuvchi nomi va parolni kiritishni so‘raydi. Natijada, shaxsiy ma’lumotlaringizni soxta saytga kiritishingiz bilan, “phishers” bu haqda darhol bilib olishadi.

Biz yuqorida aytib o‘tgan kiber tahdidlarning har biri sizning maxsus veb-saytingizga zarar yetkazishi yoki hatto butunlay ishdan chiqishiga olib kelishi mumkin. IBM ning “Ma’lumotlar buzilishining narxi” hisobotiga ko‘ra, 2020-yilda ma’lumotlar buzilishining global o‘rtacha umumiy qiymati 3,86 million dollarni tashkil etadi, bu ko‘pchilik kichik yoki o‘rta biznes uchun halokatli pul summasidir.

Endi esa onlayn kitob do‘koni portalining axborot xavfsizligini ta’minlash, tahdidlarni oldini olishning ba’zi usullarini ko‘rib chiqamiz.

1. Tizimni yangilang va ma’lumotlarni zaxiralang.

Asosiy ma’lumotlar va tizim yangilanishlarining muntazam zaxira nusxalari sizning do‘koninggiz kiberhujumga uchragan taqdirda xavfsizligini ta’minlaydi. Zaxiralash va doimiy yangilash vazifasi avtomatlashtirilishi mumkin, shuning uchun uni doimo yodda tutishingiz shart emas.

2. Internetga ulangan qurilmalaringizni shifrlang.

Mobillik davrida faqat ish stoli kompyuteridan veb-do‘konni boshqarish deyarli mumkin emas. Noutbuklar, planshetlar, smartfonlar va boshqa ko‘chma qurilmalar veb-do‘konlarni boshqarishni ancha soddalashtirdi. Biroq, xavfsizlik

hali ham yetarli darajada emas. Maxfiy ma’lumotlarni xavfsiz saqlash uchun quyidagilarni tekshirganingizga ishonch hosil qiling:

– biznes uchun foydalanadigan qurilmalar kuchli parol bilan himoyalangan;

– ularda keng qamrovli shifrlash dasturi o‘rnatilgan;

Siz barcha maxfiy ma’lumotlar yo‘qolib qolsa yoki o‘g‘irlansa, ularni o‘chirib tashlashingiz uchun qo‘l qurilmangizga masofadan turib qulflash va ma’lumotlarni o‘chirish ilovasini yuklab olishingiz lozim.

3. Parollaringizni kuchliroq qilish uchun o‘zgartiring.

Tarmoq foydalanuvchi nomi va parolni o‘zgartirishdan boshlang. Bundan tashqari, parolingizni kamida 3 oyda bir marta o‘zgartirishni davom eting. Bular parol xavfsizligi asoslari. Xuddi shu parol bilan qancha uzoq qolsangiz, uni buzish xavfi shunchalik yuqori bo‘ladi. Turli xil hisoblar uchun cheksiz sonli parollarni yo‘qotmaslik va unutmaslik uchun biz parollarni saqlaydigan va avtomatik ravishda tizimga kiradigan parol menejeri ilovalaridan foydalanishni tavsiya qilamiz, bu juda qulay. Siz sinab ko‘rishingiz mumkin bo‘lgan bir nechta echimlardan biri bu Dashlane bepul parol menejeri. Uning asosiy xususiyatlariga quyidagilar kiradi:

– parolni saqlash;

– parolning sog'lig'ini tekshirish;

– kredit karta ma’lumotlarini saqlash;

– ma’lumotlaringiz buzilgan taqdirda xavfsizlik ogohlantirishi.

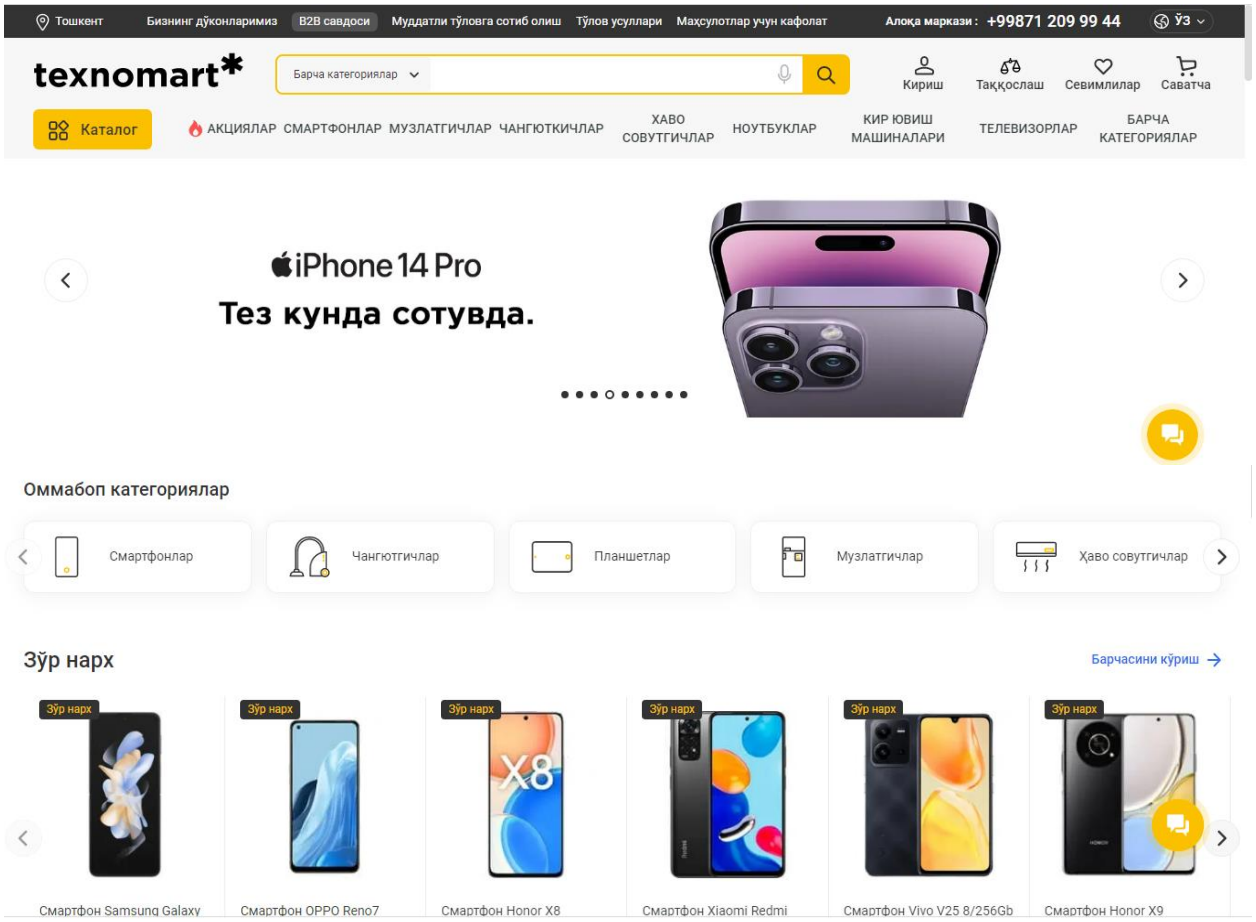
4. Veb-do‘koningizga SSL sertifikatini qo‘shing

Mijozlarning shaxsiy ma’lumotlarini himoya qilish uchun veb-do‘kon egalari har doim Secure Socket Layer sertifikatini (SSL) qo‘shadilar. SSL platformangiz va mijozlaringiz o‘rtasidagi ma’lumotlarni shifrlash uchun ishlaydi. Bu qo‘shimcha ravishda veb-saytingizning umumiy xavfsizligini oshiradi va ma’lumotlar buzilishining oldini oladi. SSL sertifikatining himoyasi manzillar panelidagi veb-saytingizning URL manzili orqali ko‘rinadi. “http://” o‘rniga “https://” veb-saytingiz SSL bilan himoyalanganligini bildiradi.

5. Masofaviy ulanishlarni himoyalash uchun VPN dan foydalaning

Bu yil ko‘pchilik masofadan ishlashni biznes egalari va xodimlar uchun foydali variant sifatida ko‘rishni boshladi. Biroq, elektron tijoratda masofaviy veb-do‘kon menejerlariga veb-sayt va boshqa muhim ma’lumotlarga kirishni ta’minlash potentsial xavfli bo‘lishi mumkin. Bu ko‘pincha xavfsizlikka ega bo‘lmagan umumiy WiFi ulanishlari kabi. Masofadan ishga olasizmi? Virtual xususiy tarmoqdan (VPN) foydalanish orqali uni xavfsiz qiling. VPN asosan qurilmaga o‘rnatilgan va yoqilganda internetga ulanishni shifrlaydigan va biznes ma’lumotlaringizga qo‘shimcha xavfsizlikni ta’minlaydigan ilovadir.

Yurtimizda reytinggi baland bo‘lgan “Texnomart.uz” onlayn savdo do‘koni ham axborot xavfsizligini ta’minlash uchun yuqorida biz ko‘rib o‘tgan usullardan



foydalanadi.

1-rasm. “Texnomart.uz” onlayn magazinining veb-sayt ko’rinishi.

Bu yerda har bir mijoz ro‘yhatdan o‘tish orqali o‘zining shaxsiy kabinetiga ega bo‘ladi va u yerda mijozning ma’lumotlari saqlanadi. Sayt xavfsizligi bilan bir qatorda mijozlarning ham ma’lumotlarini xavfsiz saqlash muhim ahamiyat kasb etadi. Shunday ekan “Texnomart.uz” onlayn do‘konlar tarmog‘i “Tarmoqlararo ekran” yoki “Firewall” lardan ham foydalaniladi. Bundan maqsad saytga tashqaridan bo‘ladigan hujumlarni to‘sish, trafikni filtrlash va begonalarning shaxsiy ma‘lumotlarga ruxsatsiz kirishini bloklash orqali axborotni xavfsizligini ta’minlashdir.

Xulosa.

Hozirgi vaqtda jahonda raqamli texnologiyalarga o‘tish jarayoni tubdan rivojlanmoqda. Hayotimizni esa internetsiz tasavvur qilib bo’lmay qoldi. Insonlar esa, ko’plab vaqtlarini manashu umumjahon o’rgimchak to’ri bilan o’tkazishga tobora odatlanib borishmoqda. Internetdan to‘g‘ri foydalanish hayotimizni oson, tez va sodda qiladi. Internet bizga shaxsiy, ijtimoiy va iqtisodiy rivojlanish uchun faktlar va raqamlar, ma’lumotlar va bilimlar bilan yordam beradi.

Internetdan foydalanish statistikasi ma’lumotlaridan quyidagilarni ko’rish mumkin:

- Internet foydalanuvchilari soni 2022-yil yanvar holatiga ko‘ra 5,1 milliard;
- Internet foydalanuvchisi har kuni o’rtacha 6 soat 43 daqiqa vaqt sarflaydi;
- 2021-yil 18-dekabrda 1,9 milliarddan ortiq veb-saytlar mavjud;
-2022 yilda global elektron tijorat chakana savdosi 5,4 trillion dollarni tashkil qilishi kutilmoqda.

Elektron tijoratdan foydalanish statistikasi [1] esa quyidagicha:

-2021-yilda elektron tijorat sotuvi 4,9 trillion dollarga yetishi kutilgan edi.

-2022-yilda global elektron tijorat chakana savdosi 5,4 trillion dollar;

-Amazon barcha onlayn sotuvlarning 49% dan ortiq bo’lib, bu Amerika Qo'shma Shtatlardagi barcha sotuvlarning taxminan 5% ni tashkil etadi.

[1] https://www.websiterating.com/research/internet-statistics-facts

Onlayn internet portallari shunday rivojlanishda davom etar ekan, uning xavfsizligiga bo‘lgan talab ham tobora ortib boradi. Onlayn veb-saytlarning xavfsizligi yuqori darajada bo‘lishi mijozlarning ham ishonchini qozonishda muhim ahamiyat kasb etadi. Axborot xavfsizligini himoya qilishdagi arzimagan xato ham onlayn veb-portalni bankrot bo‘lishiga yoki kompaniya brendining obro‘sini tushishiga olib kelishi mumkin.

Foydalanilgan adabiyotlar va internet resurslar ro‘yxati

1. O‘zbekiston Respublikasi Prezidentining Farmoni PF-5653-son “ Axborot sohasi va ommaviy kommunikatsiyalarni yanada rivojlantirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida ”gi farmoni, 02.02.2019 yildagi https://lex.uz/ru/docs/-4188795

2. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi veb-sayti. https://mitc.uz.

3. “Kiberxavfsizlik markazi” DUK rasmiy veb-sayti https://tace.uz

4. https://www.websiterating.com/ rasmiy veb-sayti.

5. Davlat axborot tizimlarini yaratish va qo‘llab-quvvatlash bo‘yicha yagona integrator https://uzinfocom.uz/