RAQAMLI TA’LIM TEXNOLOGIYALARI MARKAZI

AXBOROT XAVFSIZLIGINI TA’MINLASH BO‘LIMI

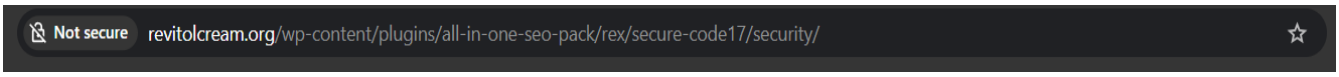
AXBOROT XAVFSIZLIGI CHORALARI

JIZZAX POLITEXNIKA INSTITUTI RAQAMLI TA’LIM TEXNOLOGIYALARI MARKAZI BO’LIMI TOMONIDAN TAVSIYA QILINADIGAN AXBOROT XAVFSIZLIGI CHORALARI

Hozirgi raqamli dunyo davrida elektron axborotlarni xavfsiz saqlash juda muhim hisoblanadi. Elektron axborotlar esa talaba malumotlari, o’qtuvchilar fayllari, reyting, baholar, testlar to’plami, shaxsiy login-parollar va boshqa malumotlar hisoblanadi. Bu malumotlarning esa o’girlab olish usulari juda ko’p hisoblanadi. Siz bu yerda sizga qilinishi mumkin bo’lgan hujumlarni oldindan bilishingiz va xavfsizlik choralarini ko’rishingiz mumkin. Asosiy hujumlardan biri bu **(1) Phishing** (soxta saytlar va dasturlar orqali malumot o’girlash) hisoblanadi. Siz bu kabi web saytlarni quyidagi yo’llar orqali aniqlab olishing mumkin:

1) **Havolasi orqali:**

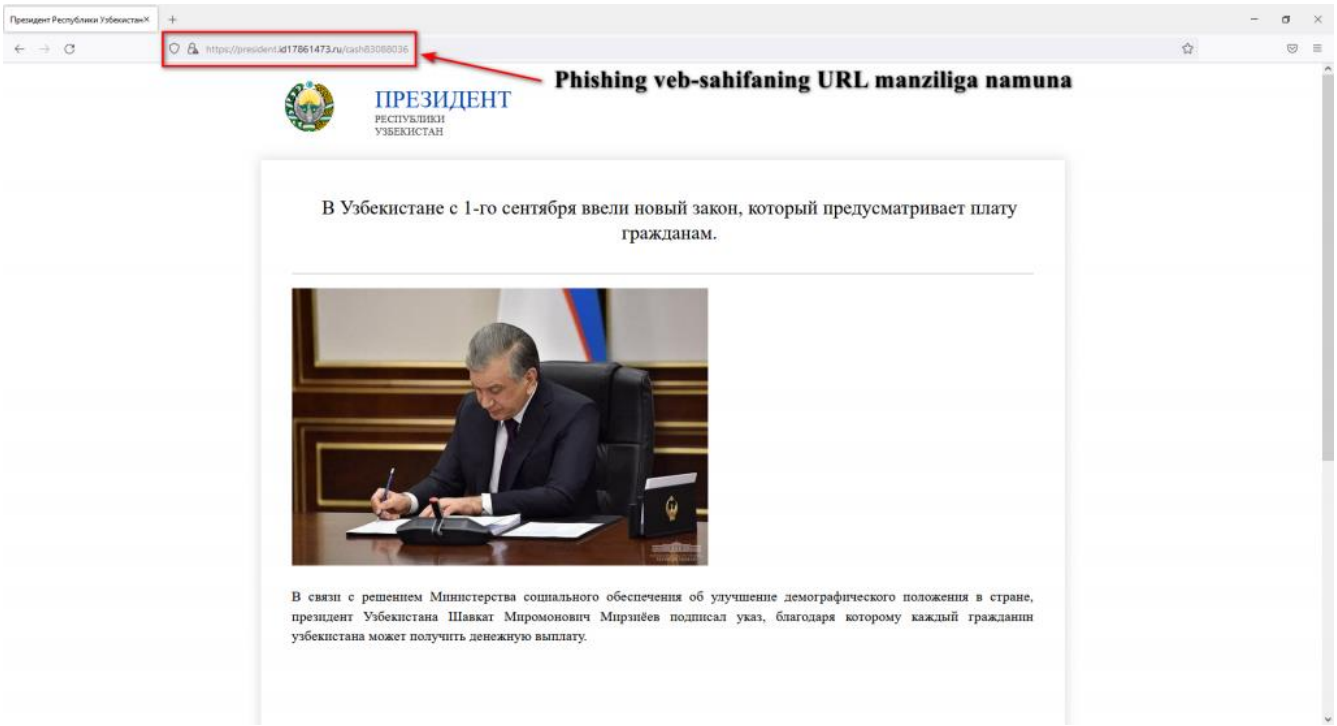
Odatda phishing web saytlarda uzun havolalar ishlatiladi

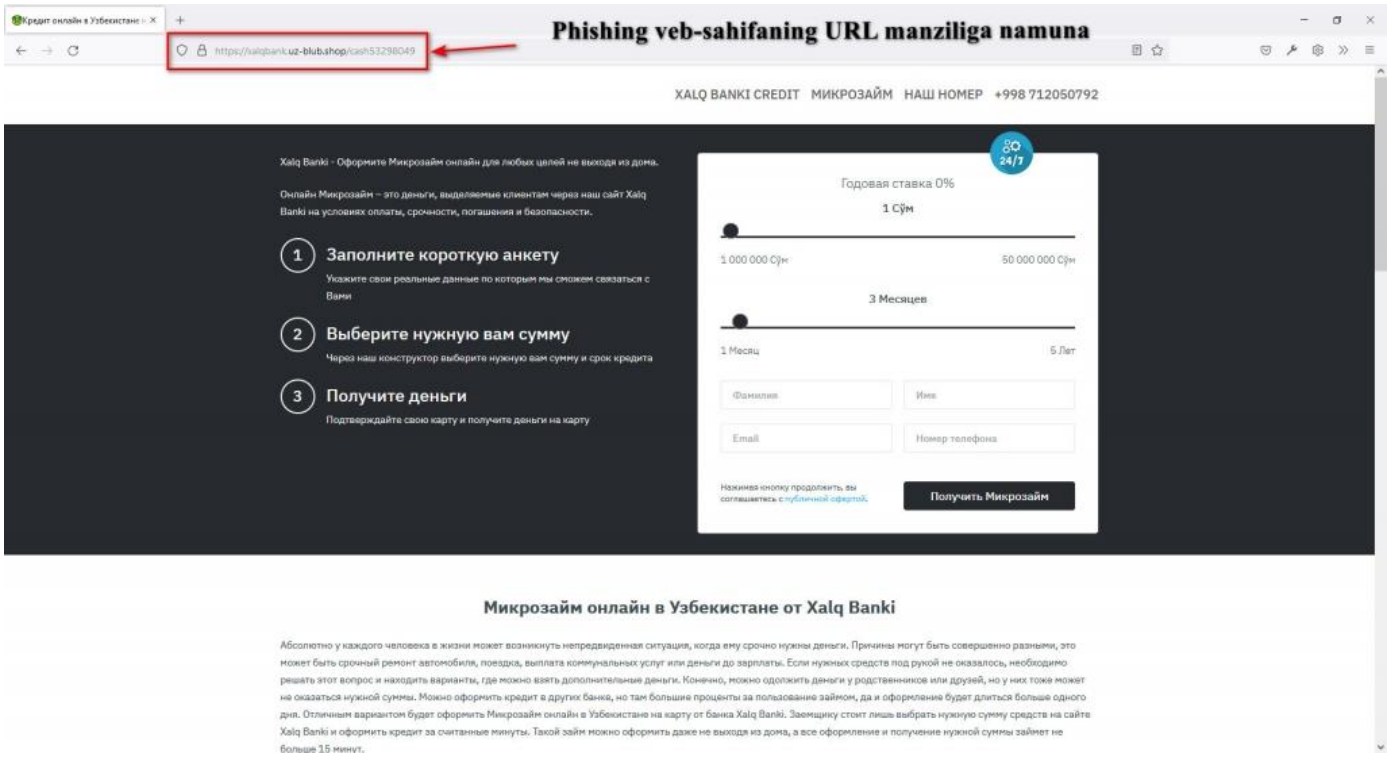


Shunday ko’rinishda bo’lishadi va siz ishlatyotgan browser orqali ogohlantirish ham berilgan bo’ladi, **“Not Secure”** so’zini ko’rishingiz mumkin. Bu yerda browser shuni aytyabdiki bu web sayt xavfsiz emas. Bunday web saytga o’xshagan web saytlarga shaxsiy (bank karta raqamlar, passport malumotlar va h.k.) malumotlarni kiritish tavsiya qilinmaydi. Bunday web saytlar orqali asosan shaxsiy malumotlaringiz olinib sotilishi mumkin yoki bank kartalaringizga ulanib online pul yichishlar amalga oshirishlari mumkin. Shuning uchun har doim qandeydir web saytga kirganingizda havolaga etibor qaratishingiz shart.

2) Mukofotlar orqali:

Inson harakteri har doim tekin narsani yoki mukofotlarni yoqitrgan va shu narsadan foyda olmoqchi bo’lgan g’araz niyatli kimsalar esa sizga banklar nomidan, mashhur brendlar nomidan sohta web saytlar ishlab chiqarib sizni pul mukofoti yutub olganingizni xabar berishadi yoki qaysidir brend 10 yilligini nishonlayotgani uchun mijozlariga pul tarqatayotganini sizga aytishadi va pulni yechib olish uchun shu havolaga kirib so’ralgan malumotlarni to’ldirishingizni so’rashadi. Shu holatda jabirlanuvchi mukofot yutdim deb o’ylab uni olish uchun to’g’ri kelgan malumotlarni kiritib yuborishi mumkin. Bu orqali esa jabirlanuvchi pulni olishni o’rniga hisobidagi barcha pulni yuqotishi mumkin.





(2) Virus va zararli dasturlar orqali ham sizni malumotlaringizni o’girlab olishi mumkin. Hozirda android va ios foydalanuvchilari ko’p bo’lgani sababli telegramda va shunga o’xshash platformalarda telefon uchun viruslar tarqatilmoqda. Ularning ko’pida sizning rasimlaringiz internetda tarqab ketibdi ko’rish uchun mana bu ilovani oching degan narsalar bo’ladi. Agar telegramda yoki boshqa social media platformasida sizga shu kabi telefon dasturlari kelsa uni ochishga hech qachon shoshilmang. Agar siz telefon ishlatyotgan bo’lsangiz va telefoningiz android bo’lsa siz uchun tavsiya qilinadigan web saytlar ro’yxati ko’rishingiz mumkin:

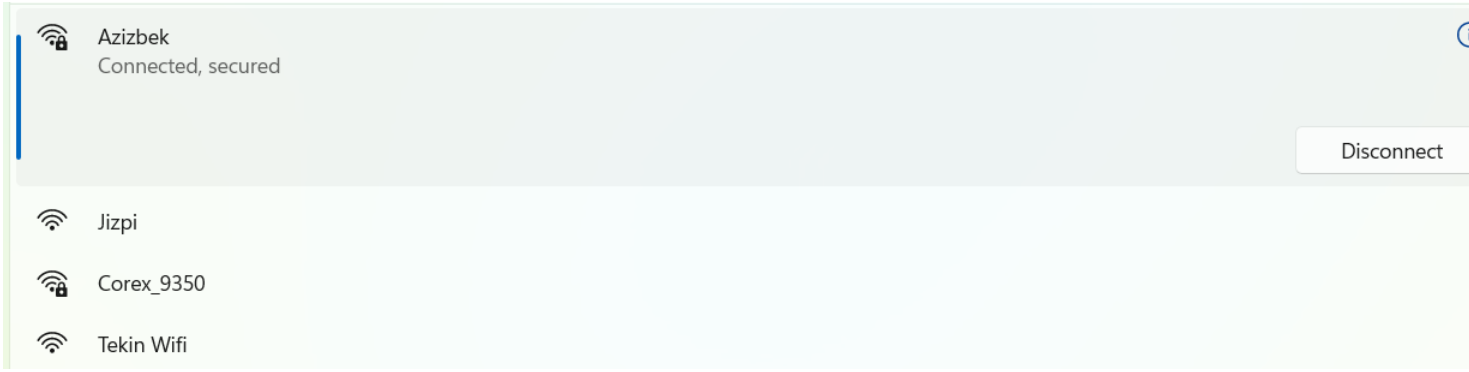
- Kaspersky Mobile Security
- BitDefender Mobile Security
- Avast Mobile Security
- Eset Mobile Security

Agar siz IOS versiyadagi telefonlarni ishlatyotgan bo’lsangiz siz bu dasturlarni o’rnatib olsangiz telefonizdagi xavfsizlik kuchayadi:

- Kaspersky security
- Avast security for IOS
- Norton Mobile Security

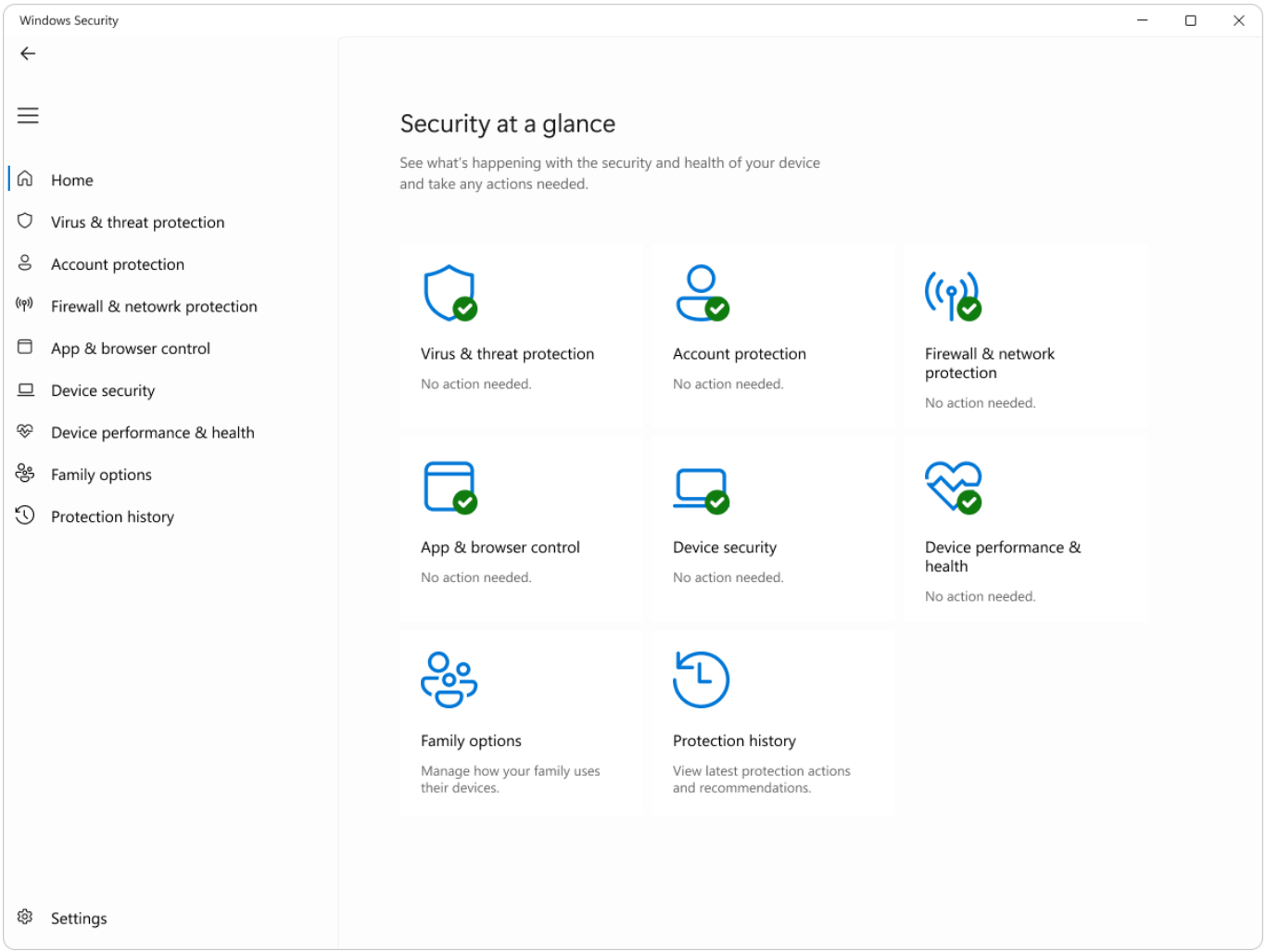
Virusdan namunani ko’rishingiz mumkin:

(3) Wifi orqali hujumlar. Ba’zi bir holatlarda wifi orqali hujumlar ham bo’lishi mumkin. U qandey sodir bo’ladi.



Ko’rib turganingizdek “**Tekin Wifi**”, u hamma uchun ochiq va ko’p hollarda internetga ulangan bo’ladi. Kop’chilik kompyuter va telefonlarda xavfsizlik o’chirlgan bo’ladi ammo telefonlorda bu holat kam uchraydi asosan kompyuterlarda ko’proq uchraydi. Siz wifiga ulanganingizda maxsus dasturlar orqali sizning tizimingizga buzib kirishadi va shaxsiy malumotlaringizni o’girlashlari mumkin. Bunday holatlardan xavfsizlikni

taminlash uchun kompyutergizda agar **“Windows”** operatsion sistemasi bo’lsa quydagi xavfsizlik yoqib quyishingiz tavsiya qilinadi.



(4) Bir xil turadagi parollarni hamma hisoblarda ishlatish. Agar sizni parolingiz hakerlar bilib olsa, u orqali parolingizni boshqa hisoblaringizda foydalanishi mumkin bo’ladi. Agar siz shu kabi xatoni takrorlagan bo’lsangiz va hakerlar tomonidan bir profilingiz olingan bo’lsa darhol boshqa profillaringizdan parolingizni almashtiring va sizning hisobingiz o’girlangan platformadagi texnik yordam bo’limidan hisobingizni vaqtinchalik muzatishlarini so’reng, vaziyat haqida malumot bering va qaytarib olganingizdan so’ng parolingizni o’zgartiring.

Xulosa qilib aytishimiz mumkin bo’lgan narsa axborot xavfsizligi har bir foydalanuvchining shaxsiy mas’uliyatidir. Raqamli ta’lim muhitida axborotlarni himoyalash bilim sifatini saqlash va shaxsiy xavfsizlikni ta’minlashning muhim omilidir. Har bir talaba va xodim yuqoridagi qoidalarga amal qilishi lozim.