# SHAXSIY MA'LUMOTLARNI HIMOYALASH

***Quldoshev Otabek Zarif o’g’li***
*kuldoshevotabek87@gmail.com*

**Annotatsiya:** Mazkur maqolada shaxsiy ma’lumotlarni qanday qilib himoyalash haqida va turli xil hozirgi vaqtdagi kiber xujumlar haqida fikr mulohazalar yuritilgan. Shuningdek, hozirgi raqamli dunyoda ma’lumotlarni qanday qilib xavfsizligini oshirish haqida muallifning umumiy xulosalari keltirilgan.

**Kalit so’zlar:** Parolni kuchaytirish, yanada xavfsiz parollarni o'rnating, ikkinchi ko'rish identifikatorlari (2FA) ni faollashtiring, shaxsiy ma'lumotlarni nazorat qiling, xavfsizlik so'rovnoma o'rnatish.

Axborot insonning 5 ta sezgi organlari orqali oladigan, cheksiz xabarlar ichidan o‘zi uchun foydali qismini xotirada saqlab qoladigan qismidir. Masalanbirov bilan tanishganda uning kiyimi, qaerda turgani, kim bilan turgani va hokazolar emas, uning ismi, qiyofasi, kasbi kabi axborotlarni eslab qolishga harakat qilinadi.

Shaxsiy ma'lumotlarni himoyalash kiberxafsizlik sohasida muhim mavzulardan biridir. Shaxsiy ma'lumotlarni himoyalash bo'yicha quyidagi maslahatlar foydali bo'lishi mumkin: Kuchli Parollar Tanlang Foydalanuvchi hisobingiz uchun kuchli va xavfsiz parollarni tanlang. Parollaringizda harflar, sonlar va belgilar kombinatsiyasini ishlatishni xohlaganingizga ishonch hosil qiling. Ikkinchi Ko'rish Identifikatorlar (2FA) Qo'llang Bir nechta faktorli autentifikatsiya protokollaridan foydalaning. Ikkinchi ko'rish identifikatorlar (masalan, SMS kodlari yoki ilova orqali amalga oshirilgan autentifikatsiya) hisobingizni qattiqroq himoyalashga yordam beradi. Foydalanilmayotgan Ma'lumotlarni O'chirish: Ehtiyotkorlik qoidalariga muvofiq, foydalanilmayotgan yoki ko'rsatilmayotgan ma'lumotlarni o'chiring. Bu, eski fayllarni, elektron pochta xabarlarni va shaxsiy ma'lumotlarni himoyalash uchun juda muhimdir. Xavfsizlik So'rovnoma Dasturlaridan Foydalaning: O'rnatilgan xavfsizlik so'rovnoma dasturlarini (masalan, antivirus dasturlar) o'rnating va yangilanishlarni avtomatik ravishda tekshiring. Shifrlash Teknologiyalaridan Foydalaning: E-mail va fayllarni shifrlang. Masalan, End-to-End shifrlash protokollaridan foydalaning va ma'lumotlarni xavfsiz tarzda almashishingizga ishonch hosil qiling. Internet Bog'lanishlarini Xavfsizlashtiring: Umuman, internet bog'lanishlarini xavfsizlashtiruvchi protokollardan foydalaning, masalan, HTTPS yoki VPN. Ma'lumotlarni Redda Qiling: Foydalanayotgan veb-saytlardagi cookieslarni va tarixni red eting. Bunday ma'lumotlarni boshqa shaxslar bilan o'zaro almashish jarayonini cheklash uchun kerakli bo'lmagan ma'lumotlarni saqlang.

Bilim Olish: Shaxsiy ma'lumotlarni himoyalash sohasida yangiliklar va rivojlanayotgan xavfsizlik texnologiyalari haqida ma'lumotlarni o'rganing. Bu, sizning ma'lumotlaringizni himoyalash va xavfsizlikni oshirishga yordam beradi. Yaxshi Odatlarni O'rganing: Shaxsiy ma'lumotlarni himoyalash uchun yaxshi odatlarni o'rganing va ularni amalga oshiring. Masalan, hamma vaqt uchun shifrlash, ushbu ma'lumotlarga faqat ishonch hosil qilgan tashrif buyuruvchilar bilan ulanishingiz. Ma'lumotlaringizni Ko'chirishdan Chidamlaning: Ma'lumotlaringizni juda ko'p o'rgatishdan chidamlaning. Har doim kerakli bo'lmagan ma'lumotlarni o'chirib tashlash yoki boshqalarga topshirishni, o'z ma'lumotlarining yo'naltirishini qisqaritib turish. Parollarni Xavfsiz Tashlash: Kuchli va xavfsiz parollar ishlatish juda muhimdir. Parollaringizda harflar, sonlar va belgilar kombinatsiyasini ishlatishni unutmang. Ikkinchi Ko'rish Identifikatorlardan (2FA) Foydalaning: Ikkinchi ko'rish identifikatorlardan foydalaning, masalan, SMS kodlari yoki ilova orqali amalga oshirilgan autentifikatsiya. Bu, hisobingizni qattiqroq himoyalashga yordam beradi. Ma'lumotlarni Shifrlang: Shifrlash tekhnologiyalaridan foydalaning, masalan, End-to-End shifrlash protokollari. Bu, ma'lumotlaringizni xavfsiz tarzda almashishingizga yordam beradi. Foydalanilmayotgan Ma'lumotlarni O'chirish: Foydalanilmayotgan yoki ko'rsatilmayotgan ma'lumotlarni tozalang. Eski fayllarni va elektron pochta xabarlarni tozalash juda muhim. Xavfsizlik Dasturlaridan Foydalaning: O'rnatilgan xavfsizlik dasturlarini (antivirus dasturlar va xavfsizlik so'rovnoma dasturlari) o'rnating va yangilanishlarni avtomatik ravishda tekshiring. Shaxsiy Xabarlar Va Foydalanish Tarixini Nazorat Qiling: Internetda foydalanayotgan xabarlar va foydalanish tarixingizni nazorat qiling. Foydalanish tarixingizni tozalab tashlang va iltimos, shaxsiy ma'lumotlaringizni foydalanayotgan saytlarga etibor bering. Kiberxafsizlik Sohasida O'z Bilimini Oshiring: Kiberxafsizlik sohasida o'z bilimingizni oshiring va xavfsizlikni oshirish uchun yangiliklarni kuzating. Internet Bog'lanishlarini Xavfsizlashtiring: Internet bog'lanishlarini xavfsizlashtiring. Masalan, HTTPS yoki VPN protokollari orqali bog'laning. Foydalanish Sayt Va Ilmoy Saytlarning Maxfiylik Siyosatini O'rganing: Sizning foydalanayotgan saytingiz va ilmoy saytlar sizning ma'lumotlaringizni qanday qilib saqlashadi haqida o'zingizni tushunishingiz muhim. Xavfsizlikni Tez-tez Nazorat Qiling: Xavfsizlik sohasidagi yangiliklarni va o'zgarishlarni nazorat qilish juda muhim. Sizning amalga oshirilayotgan ilovalaringiz va platformalaringizni doimo yangilab turib, eng so'nggi xavfsizlik maslahatlari va usullaridan foydalaning.

Yana bir hozirgi kunda keng tarqalgan ijtiomoiy tarmoqlar hisoblanadi. Biz nima qilishimiz kerak? Agar siz ham ijtimoiy tarmoqlarda ko’p vaqt o’tkazadigan odamlar qatorida bo’lsangiz, siz Internetda juda ko’p shaxsiy ma’lumotlaringizni qoldirishingiz ehtimoli juda yuqori. Turli xil ijtimoiy tarmoqlardagi akkauntlarimizda biz ko’pincha

juda ko’p shaxsiy tafsilotlarni oshkor qilamiz, masalan, ism-sharifimiz, o’qish yoki ishlash joyimiz, oila a’zolarimiz va do’stlarimiz, manzilimiz yoki tez-tez borib turadigan joylarimiz, qiziqish va sevimli mashg’ulotlarimiz, siyosiy qarashlarimiz va yoqtirgan musiqamiz va hokazo.

Bu ma’lumotlarning barchasidan o‘zimizga qarshi ishlatilishi mumkin. Firibgarlar sizning shaxsiy ma’lumotlaringizdan foydalanib sizning nomingizdan ish tutishlari, do’stlaringiz yoki hamkasblaringizdan pul yoki maxfiy ma’lumotlarni olish maqsadida ma’lumotlaringizdan ularni aldash uchun foydalanishi mumkin. Ular ijtimoiy tarmoqlardagi akkauntlaringizdan olingan ma’lumotlardan bank tizimlari yoki tanishuv saytlaridagi xavfsizlik nazorati savollariga javoblarni taxmin qilib topish, onlayn akkauntlaringizni o‘g‘irlash yoki sizni taqib qilish uchun foydalanishlari mumkin.

Lekin ijtimoiy tarmoqlardan foydalanishdan voz kechishingiz shart emas, quyida biz ijtimoiy tarmoqlarda shaxsiy ma’lumotlaringizni xavfsiz saqlashga yordam beradigan bir nechta tez va oson yechimlar haqida ma’lumot beramiz. 1. Kuchli va takrorlanmas parollardan foydalaning

Har bir ijtimoiy tarmoq akkauntingizni taxmin qilib topib bo’lmas yoki buzib bo’lmas parol bilan himoyalang. Kamida 12 ta belgidan, jumladan katta va kichik harflar, raqamlar va maxsus belgilardan iborat bo’lgan parol kuchli hisoblanadi. Ushbu belgilarning tasodifiy birikmasidan tashkil topgan parol eng kuchli hisoblanadi. Qanday qilib buzish qiyin bo’lgan ishonchli va murakkab parollar yaratish haqida bu yerda batafsil o’qing.

Har bir onlayn akkauntingiz uchun takrorlanmas paroldan foydalaning. Nima uchun turli akkauntlar uchun bir xil yoki o‘xshash paroldan foydalanish noto’g’ri fikr ekanligi haqida bu yerda batafsil o‘qing. Qiyin va takrorlanmas parollarni yodda saqlash haqida bosh qotirmasangiz ham bo’ladi. Ularni «eslab qolish» va xavfsiz saqlash uchun Parol Menejeridan foydalanishingiz mumkin.

Ikkinchi himoya qatlamini qo‘shing. Afsuski, hatto eng kuchli parolni ham o’g’irlash yoki buzib kirilishi mumkin. Shuning uchun siz ijtimoiy media akkauntlaringizni himoyalash uchun ikki faktorli autentifikatsiyadan (2FA) foydalanishingiz kerak. Ikki faktorli autentifikatsiyadan (2FA) foydalanish parol kiritishdan tashqari, qo’shimcha tarzda shaxsingizni tasdiqlashingiz kerakligini anglatadi. 2FA dan foydalanishning eng xavfsiz usuli bu sizning smartfoningizga vaqtinchalik raqamli kodlarni yaratib beruvchi ilovani o’rnatishdir. Ijtimoiy tarmoq akkauntiga kirish uchun parolni kiritganingizdan so’ng darhol bunday kodni kiritishingiz kerak bo’ladi. Onlayn akkauntlarni himoyalash uchun ikki faktorli autentifikatsiyadan (2FA) qanday foydalanish haqida batafsil o‘qing.

Dasturiy ta’minotni muntazam ravishda yangilab boring. Kiberjinoyatchilar odamlarning qurilmalariga o‘rnatilgan turli ilovalardagi zaifliklardan tobora yaxsiroq foydalanayotgan bir paytda dasturiy ta’minotni yangilab turish juda muhim. Ijtimoiy media akkauntlaringizga kirish uchun foydalanayotgan qurilmangiz operatsion tizimi har doim eng so’nggi versiyaga albatta yangilangan bo’lsin. Kompyuter yoki mobil qurilmadan foydalanishda antivirusning yoqilganligi va avtomatik yangilashga sozlanganligiga ishonch hosil qiling. Agar siz ijtimoiy tarmoqlarga ilova orqali emas, balki brauzer orqali kirsangiz, uning so‘nggi versiyaga yangilanganligiga amin bo’ling. Agar siz mobil qurilmada maxsus ijtimoiy media ilovalaridan foydalansangiz, ularni tez-tez yangilab turing. Ijtimoiy tarmoqlarda faqat tanigan odamlar bilangina do’st bo’ling. Hammasi juda oddiy: siz qanchalik ko’p odamlar bilan ijtimoiy tarmoqlarda bog’lansangiz, siz bo’lishgan shaxsiy ma’lumotlaringizni nazorat qilish shunchalik qiyin bo’ladi. Agar ijtimoiy tarmoqlardagi akkauntlaringizni hamma uchun ochiq saqlashga jiddiy sabab bo’lmasa, sizning postlaringiz va fotosuratlaringizni ko’ra oluvchi foydalanuvchilar doirasini cheklaganingiz ma’qul. Buni Instagram va Twitter tarmoqlarida qanday sozlash haqida batafsil o‘qing. Siz foydalanadigan ijtimoiy media xizmatlarida sizni kuzatib boruvchi foydalanuvchilar ro’yxatini muntazam ravishda qayta ko’zdan kechirib boring. Siz hozirda ishonmaydigan yoki ular bilan muloqot qilmaydigan odamlarni do’stlaringiz qatoridan o’chiring. Agar biror-bir foydalanuvchi sizdan shaxsiy ma’lumotlaringizni so‘rasa, bezovta qilsa yoki boshqa shubhali harakatlarni sodir etsa, uning profilini bloklang va ustidan shikoyat qiling. Maxfiylik sozlamalarini sozlang. Ijtimoiy media xizmatlari sizning post va fotosuratlaringizni butun dunyo bo’ylab imkon qadar ko’proq foydalanuvchilarga ochiq qiladigan qilib sozlangan. Yaxshiyamki, ushbu xizmatlar sizga standart maxfiylik sozlamalarini o’zgartirishga imkon beradi, ya’ni siz boshqalar qancha ma’lumotlaringizni ko’rishini aniq nazorat qilishingiz mumkin. Masalan, ko’p ijtimoiy tarmoqlar sizga profilingizni kim ko’rishini cheklash, ma’lum foydalanuvchilarni bloklash, fotosuratlarni faqat ma’lum odamlar bilangina bo’lishish kabi sozlamalarni o’rnatish imkonini beradi. Bu sozlamardan to’g’ri foydalanishni albatta yaxshilab o’rganing va maxfiyligingizni maksimal darajada oshirish uchun ularni to’g’ri boshqaring. Instagram va Twitter tarmoqlarida maxfiylik sozlamalarini qanday boshqarish haqida batafsil o’qing. Ijtimoiy tarmoqlarda shaxsiy ma’lumotlaringizni saqlamang

Ijtimoiy media saytlari siz haqingizda boshqalar ko’proq ma’lumot topa olishini osonlashtirishdan manfaatdor. Qayerda o‘qigansiz? Oilalimisiz? Bizning tarmog’imizda yana qaysi oila a’zolaringizning akkaunti bor? Bunday savollarga olingan batafsil javoblar orqali ijtimoiy media saytlari sizning hayotingizning juda yaqqol tasvirini boshqalarga beradi, ya’ni g’araz niyatli odamlar uchun bu bebaho ma’lumotlardir. Biografik ma’lumotlar, oilaviy aloqalar va fotosuratlar kabi ijtimoiy

tarmoqlarda joylashtirgan shaxsiy ma’lumotlaringiz miqdorini cheklashga harakat qiling. Hech qachon shaxsiy guvohnomalaringiz, konsert chiptalari yoki transport bortiga chiqish talonlaringiz fotosuratlarini ijtomoiy tarmoqlarda bo’lishmang. Oz’ingiz mulohaza qiling va yodda tuting, tarmoqlarda joylashtirgan ma’lumotlaringizni bekor qilish yoki ularga aynan kimlar kirish huquqiga ega ekanligini bilish deyarli imkonsiz. Lokatsiyani (joylashgan manzil) bo’lishmang

Ijtimoiy tarmoq foydalanuvchilari ko’pincha har kimga qayerda ekanligi va qayerga borishlarini aytish orqali o’zlarini yomon niyatli odamlarning oson nishoniga aylantiradi. Foydalanuvchilar ijtimoiy media ilovalarida lokatsiyani belgilash funksiyasidan foydalanish, qayerda ekanliklarini ko‘rsatuvchi fotosuratlarni joylashtirish yoki biror joyda o’tkazayotgan ajoyib vaqtlari haqida tarmoqlarda yozish orqali o’z lokatsiyalarini bo’lishadilar. Agar siz uchun maxfiyligingiz va shaxsiy xavfsizligingiz muhim bo‘lsa, lokatsiyangizni ijtimoiy tarmoqlarda boshqalar bilan bo’lishmaganingiz ma’qul. Gadjetingizning lokatsiyani ulashish funksiyasini o‘chirib qo‘ying va sizning lokatsiyangizni kuzata olmasliklari uchun ijtimoiy tarmoqlardagi maxfiylik sozlamalarini sozlang. Ijtimoiy tarmoqda lokatsiyangizni belgilamang va qayerda ekanligingiz yaqqol ma’lum bo’lgan fotosuratlarni u yerda hali bo’lib turgan vaqtingizda joylashtirmang. Ijtimoiy tarmoq profilingizdan boshqa saytlarga kirish yoki ro’yxatdan o’tish uchun foydalanmang

Biror bir servisda yoki internetdagi yangi platformada navbatdagi akkauntni yaratishda «Facebook orqali kirish» funksiyasidan foydalanish qulay va oson tuyulishi mumkin. Biroq bunday yo’l tutishingiz, siz uchinchi tomon saytiga Facebook akkauntingiz ma’lumotlarini ishonishingizni anglatadi. Oddiy statistik nuqtai nazardan qaralganda ham, bu sizning akkauntingiz buzilishi ehtimolini oshiradi. Bundan tashqari, siz Facebook tarmog’iga ham yanada ko’proq shaxsiy ma’lumotlaringizga kirishni topshirasiz. Shuning uchun, hech qachon ijtimoiy media akkauntlaringiz bilan boshqa veb-saytlarga kirish yoki ro’yxatdan o’tish uchun foydalanmang. Boshqa ilovalarga akkauntingizga kirish huquqini bermang

Aksariyat foydalanuvchilar qancha ilova yoki veb-saytlarni o’z ijtimoiy media akkauntlariga bog’laganlarini hattoki bilmaydilar. Har safar siz Facebook tarmog’ida kimdir siz bilan bo’lishgan testni bosganingizda, yoki “Qaysi mashhur odamga o‘xshashingizni ko‘rish uchun bu yerga bosing” havolasiga kirganingizda, yana bir qo‘shimcha ilova yoki xizmatga akkauntingizga kirish huquqini berasiz. Ushbu ilovalar do’stlaringiz ro’yxati, profil rasmlaringiz, tug’ilgan sana va manzilingiz kabi ma’lumotlaringizni ko’ra olishi mumkin. Ijtimoiy tarmoq akkauntlaringizga kirish huquqiga ega bo’lgan ilova va xizmatlar ro’yxatini muntazam ravishda ko’zdan kechiring. Eskirgan, shubhali yoki keraksiz barcha xizmat va ilovalarni o’chirib tashlang. Umumiy va jamoat (jamoat joylaridagi) qurilmalaridan to’g’ri foydalanishni

biling. Umumiy yoki jamoat qurilmalarida (jamoat joylaridagi) ijtimoiy media akkaunlariga kirish har doim shaxsiy ma’lumotlaringizni xavf ostiga qo’yadi. Ushbu xatarlarning ba’zilarini kamaytirish mumkin bo’lsa-da, ularni butunlay bartaraf qila olmaysiz. Ijtimoiy media profillaringizni tekshirish uchun kutubxona, maktab yoki aeroportdagi jamoat qurilmalaridan foydalanganingizda, har doim tizimdan chiqishni unutmang va iloji bo’lsa, seansni tugating yoki qurilmani qayta ishga tushiring. Iloji bo’lsa, internet-kafelardagi umumiy foydalanish kompyuterlarida ijtimoiy tarmoqlardagi akkauntlaringizga kirmang. Har doim bunday kompyuterlarda keyloggerlar yoki boshqa turdagi josuslik dasturlari o’rnatilgan deb hisoblang. Agar Internet-kafeda ijtimoiy tarmoq akkauntingizga kirish zarur bo’lsa, akkauntingizni himoyalash uchun ikki faktorli autentifikatsiyani (2FA) yoqing va foydalanib bo’lgandan so’ng imkon qadar tezroq boshqa kompyuterdan ushbu akkaunt parolini o’zgartiring. Havolalardan foydalanishda e’tiborli bo’ling. Raqamli xavfsizlikning asosiy qoidalaridan biri bu – siz tanimaydigan yoki to‘liq ishonmaydigan odamlarning havolalarini hech qachon bosmasligingiz kerak. Bu qoida ijtimoiy tarmoqlardagi havolalarga nisbatan ham qo‘llaniladi. Bunday zarari havolalar sizga shaxsiy xabarlar orqali yuborilishi yoki ijtimoiy tarmoqda fotosurat yoki status yangilanishi ostidagi sharhlarda joylashtirilgan bo’lishi mumkin. Agar havola sizni qanday saytga olib borishini aniq bilmasangiz, uni bosmaganingiz maqul. Havola ustiga sichqonchani olib kelsangiz, (sichqoncha tugmasini bosmang) havola bosilsa, qanday saytga olib borishi haqida ko‘proq ma’lumot brauzer oynasining pastki qismida namoyon bo’ladi. Afsuski, bu imkoniyat mobil qurilmalarda mavjud emas.

Keraksiz akkauntlarni yoping. Yangi va zamonaviy ijtimoiy media platformalar eskirgan platformalar o’rnini egallar ekan, siz ochgan barcha akkauntlaringizni ko’zdan kechirish va ortiq foydalanmayotganlaringizni o‘chirib tashlashingiz juda muhim. Xakerlar uchun sizning tashlab qo’yilgan yoki esdan chiqargan akkauntlaringizni sezdirmasdan buzish osonroq. Xakerlar buzilgan akkauntingizdagi ma’lumotlardan foydalanib boshqa akkauntlaringizni ham buzib kirishi yoki ko’proq ma’lumot uchun o’zlarini sizning qiyofangizda ko’rsatishlari mumkin. Siz keraksiz akkauntlaringizni yopishdan tashqari, iloji bo’lsa, ijtimoiy media xizmatidan ularda mavjud barcha ma’lumotlaringizni o’chirib tashlashni so’rang. Parol manajeridan foydalanishning afzalliklaridan biri – u ochgan barcha akkauntlaringizni kuzatishni osonlashtiradi.

## Xulosa

Agar siz tanimagan, bilmagan insonlarga ma’lumotlaringizni oshkor qilmang. Shaxsiy qurilmangizni boshqalarga bermang, karta ma’lumotlarini, shaxsni tasdiqlovchi ma’lumotlarni o’zingiz bilmagan insonlarga bermang. Qachonki ishonchingiz komil bo’lgandagina bersangiz bo’ladi.

## Foydalanilgan adabiyotlar

1 Kim David. Fundamentals of Information Systems Security. -USA, 2014 - p.544.
2 Mark Stump. Information Security: principles and practice. -2 2011 -p.608.
3 Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. -Т.: Ўзбекистон маркаси, 2009 -432 б.
4 Пардаев А.Х. ва бошқалар. Ахборот хавфсизлиги: муаммо ва ечимлар. -Т.:Ёзувчи, 2004
5 Мамаев М., Петренко С.. Технологии защиты информации в интернете. -С/П:Питер, 2002 -844 с.
6 Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. -М.:Полигон-АСТ, 2000 -270 с.
7 Шнайер Б. Секреты и ложь: безопасность данных в цифровом мире. -С/П: Питер, 2003 -368 с.
8 Под рук. Сонникова В.Г. Технические методы и средства защиты информации. -М.: Полигон-АСТ, 2000 -314 с.
9 Ibragimov R.I., Tulaganova Z.X., Mamurova F.I., Boltayev A.X. «Axborot xavfsizligi va axborotni himoyalash» fani bo’yicha laboratoriya ishlari to’plami. -T.: ToshTYMI, 2011 -55 b.
10. https://cyber-star.org/