

IJTIMOIIY TARMOQLARDA XAVFSIZLIK MUAMMOLARI

Hafizov Shukrullo Fayzullo o'g'li

Oripov Asilbek Baxtiyor o'g'li

Saidov Ozodbek Alisher o'g'li

O'ktamov Doston Rustam o'g'li

Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: Mazkur maqolada ijtimoiy tarmoqlarda yuzaga kelayotgan xavfsizlik muammolari va ularning foydalanuvchilarga ta'siri tahlil qilingan. Xususan, shaxsiy ma'lumotlarning tarqalishi, kiberhujumlar, fishing, soxta akkauntlar, kiberbulling va zararli kontent kabi tahdidlar yoritib berilgan. Shuningdek, ijtimoiy tarmoqlarda axborot xavfsizligini ta'minlash, maxfiylikni himoya qilish hamda foydalanuvchilarning raqamli savodxonligini oshirish masalalari ko'rib chiqilgan.

Kalt so'zlar: *Ijtimoiy tarmoq, internet, ijtimoiy tarmoq tahlili (ITT), tugun, qirra, markazlik, tarmoq zichligi, klasterlash, kichik dunyo fenomeni, axborot almashish, onlayn muloqot, maxfiylik, raqamli kommunikatsiya.*

Ijtimoiy tarmoqlar bugungi dunyoda juda mashhur. Millionlab odamlar ijtimoiy tarmoqlarning turli shakllaridan foydalanadilar, chunki ular odamlarga do'stlari va oilalari bilan bog'lanish, shaxsiy ma'lumotlarni almashish imkonini beradi.

Biroq, foydalanuvchi tomonidan yuklangan kontent fotosuratlar, videolar va audiolar kabi multimedia bo'lsa ma'lumotlarining maxfiyligi va xavfsizligini ta'minlash bilan bog'liq muammolar yuzaga kelishi mumkin.

Yuklangan multimedia kontenti ijtimoiy tarmoq ichida va undan tashqarida virusli va deyarli bir zumda uzatilishi mumkin bo'lgan ma'lumotlarni o'z ichiga oladi.



1.1-rasm Ijtimoiy tarmoq qulayliklari keltirilgan rasm

Facebook kabi ko'pgina Ijtimoiy tarmoq xavfsizliklarda asosan multimedia ma'lumotlari ishlab chiqariladi va almashiladi. SocialMediaToday statistik ma'lumotlari shuni ko'rsatadiki, Facebookda videolarning o'rtacha ko'rish va almashish tezligi kundan-kunga oshib bormoqda. Ayni paytda Facebook'da kuniga taxminan 8 milliard video ko'rilmoqda, bu 2015-yilda ko'rilganidan ikki baravar ko'p. Facebook'da mavjud bo'lgan multimedia ma'lumotlarining ko'pligi tufayli xavfsizlik xatarlari ham ortib bormoqda. Zararli foydalanuvchi zararli ma'lumotni multimedia ma'lumotlari ichida yashirish orqali ijtimoiy tarmoqda baham ko'rishi mumkin. Bundan tashqari, bu orqali tajovuzkor foydalanuvchining identifikatori va joylashuvi kabi muhim ma'lumotlarni osongina topishi mumkin.

Twitter kabi ba'zi Ijtimoiy tarmoqlar foydalanuvchilarga muhim shaxsiy ma'lumotlarni oshkor qilishga ruxsat bermaydi, biroq tajovuzkorlar foydalanuvchining ijtimoiy tarmoqlarda joylashtirgan kontenti ketma-ketligini taxmin qilishlari va ularning oshkor etilmagan shaxsiy ma'lumotlarini ochishlari mumkin. 2005 yilda MySpace-ga Sammy worm (qurti) hujum qildi, u MySpace-dagi zaifliklardan foydalangan va juda tez uzatilgan. U foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlamadi, lekin MySpace'ning umumiy faoliyatiga xavfli ta'sir ko'rsatdi. 2009 yil aprel oyida Twitter Mikeyy qurti tomonidan hujumga uchradi, u ham foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlamadi, balki ularning ma'lumotlarini ba'zi yaroqsiz ma'lumotlar bilan almashtirdi. 2009-yil may oyida Facebook'ga Koobface qurti hujum qildi, u foydalanuvchi paroli kabi muhim ma'lumotlarni o'g'irladi.

Internet xavfsizligiga tahdid hisoboti (ISTR) ta'kidlaganidek, xakerlar tomonidan ijtimoiy tarmoqlardan ko'proq foydalanishni e'tiborsiz qoldirib bo'lmaydi. 2015-yilda bunday xizmatlar spam va zararli dasturlar uchun manbaga aylandi va Internetda noqonuniy pul ishlash usuli sifatida foydalanildi. Yaqinda Facebook bosh direktori Mark Sukerbergning Pinterest va Twitter akkauntlari xakerlik hujumiga uchradi, bu yerda xaker o'zining LinkedIn-dagi "dadada" parolidan foydalangan. Xuddi shunday, tajovuzkorlar Delta Air Lines Inc. va Newsweek kompaniyalarining Ijtimoiy tarmoq akkauntlariga soxta xabarlarini joylashtirish orqali kirib kelgan.

Ijtimoiy tarmoqlardagi multimedia ma'lumotlari tufayli an'anaviy tahdidlar soni ortib borayotganligi sababli ko'plab tadqiqotchilar va xavfsizlik korporatsiyalari ushbu tahdidlarni yumshatish uchun turli yechimlarni taklif qilmoqda. Bunday yechimlarga ijtimoiy tarmoq foydalanuvchilarini multimedia ma'lumotlari tufayli tahdidlardan himoya qilish uchun suv belgilari (watermarking), stegonaliz va raqamli unutish kiradi. Boshqa tomondan, an'anaviy tahdidlarni yumshatish uchun spamni aniqlash va fishingni aniqlash kabi turli xil yechimlar taklif qilingan. Biroq, autentifikatsiya mexanizmlari va maxfiylik sozlamalari kabi ko'plab o'rnatilgan xavfsizlik yechimlari va kichik monitor va ijtimoiy himoya ilovasi kabi tijorat yechimlari ham har ikki turdagi xavfsizlikka qarshi himoya vazifasini bajaradi.

Xavfsizlik bo'yicha ko'plab tadqiqotchilar Ijtimoiy tarmoqdagi xavfsizlik masalalarini o'rganib chiqdilar va muhokama qildilar. Gao va boshqalarning [8] tadqiqoti ijtimoiy tarmoqdagi asosiy xavfsizlik muammolarini to'rt toifaga ajratdi:

- Maxfiylik muammolari;
- Virusli marketing;
- Tarmoq strukturasiga asoslangan hujumlar;
- Zararli dasturiy ta'minot hujumlari.

Bundan tashqari, u eng yangi xavfsizlik yechimlarining yuqori darajadagi taksonomiyasini taqdim etadi.

Internet tahdidlari - Foydalanuvchilar ijtimoiy tarmoqlarda katta hajmdagi shaxsiy ma'lumotlarni baham ko'rishadi va bu ma'lumotlar ularni shaxsiy ma'lumotlarni o'g'irlash, spam yuborish, fishing, onlayn yirtqichlar, internet-firibgarlik va boshqa kiberjinoyatchilik hujumlari kabi turli internet tahdidlariga duch kelishi mumkin. 2016-yildagi Internet xavfsizligiga tahdidlar hisobotiga ko'ra ijtimoiy tarmoqlar shaxsiy ma'lumotlarni o'g'irlash uchun hujumchilarning eng istiqbolli nishoniga aylandi. Ushbu turdagi hujumda tajovuzkor foydalanuvchining ijtimoiy himoya raqami, to'liq ismi, telefon raqami va manzili kabi maxfiy ma'lumotlaridan uning ruxsatisiz o'g'irlik yoki firibgarlik kabi kiberjinoyatlarni amalga oshirish uchun foydalanadi. Hozirgi vaqtda ko'pgina Ijtimoiy tarmoqlarning standart maxfiylik xususiyatlari, ular butun foydalanuvchining shaxsiy ma'lumotlarini hamma uchun ochiq bo'lishini belgilaydi. Shu sababli, tajovuzkor shunchaki foydalanuvchining do'stlari haqidagi ma'lumotlarga kirishi va keyin o'zini ishonchli do'st sifatida ko'rsatishi mumkin. Bundan tashqari, tajovuzkor foydalanuvchini qo'shimcha tijorat va maxfiy ma'lumotlarni talab qilishga ko'ndira oladi. Bundan tashqari, ijtimoiylarda fishing hujumi tendentsiyasi 2007-yilda boshlangan. Ushbu hujumda raqiblar foydalanuvchining shaxsiy ma'lumotlaridan foydalanib, uning ijtimoiy tarmoqda baham ko'rgan moliyaviy ma'lumotlarini olishga harakat qiladilar. G'arazli maqsaddagi insonlar shuningdek, mashhur odamlarning ijtimoiy tarmoq akkauntlariga kirishi va keyin do'stlari bilan muloqot qilish uchun ushbu akkauntlardan foydalanishi mumkin. Bundan tashqari, ijtimoiy tarmoqlarda uchinchi tomon dasturlaridan foydalanish ham katta xavfsizlik tahdidi sifatida ishlaydi. Misol uchun, Facebook Instagram kabi ko'plab ijtimoiy tarmoqlar o'z foydalanuvchilariga o'yin ilovalarini taqdim etadi. Ushbu ilovalar foydalanuvchining kredit karta ma'lumotlarini, shaxsiy ma'lumotlar, masalan: telefon raqami va ro'yxatdan o'tish jarayonini yakunlash uchun elektron pochta identifikatori. O'zining telefon raqami va kredit karta ma'lumotlarini taqdim etgan foydalanuvchi identifikatorni o'g'irlash va fishing xavfini oshirishi mumkin.

Obro' va ishonch bilan bog'liq muammolar. Obro' bu shaxs, birlashma yoki bir guruh odamlarning jamoaviy bahosining bir turi. Bu korporativ, ijtimoiy maqom,

onlayn guruhlar kabi ko'plab sohalarda muhim rol o'ynaydi. Ko'p odamlar o'z hayotlarini yozib olish va do'stlari bilan aloqada bo'lish uchun ijtimoiy tarmoqlarga tayanadilar. Bundan tashqari, ijtimoiy tarmoqlar foydalanuvchining do'stlari doirasidan tashqarida ko'rishlar, videolar va rasmlarni almashish uchun ishlatilishi mumkin. Ijtimoiy tarmoqlardan yuqori darajada foydalanish bilan foydalanuvchilarning onlayn obro'si ham internet orqali tezlashadi. Keyinchalik, foydalanuvchilarning obro'si ham foydalanuvchining holati va haqiqiy hayotdagi ishonchliligiga ta'sir qiladi. Ijtimoiy tarmoqlar korxonalar va yirik tashkilotlarning obro'siga putur yetkazishi mumkin, bunda kompaniyaning biron bir xodimi bitta o'ylamasdan xabar yuborsa, bu xodim va kompaniyaning obro'siga putur yetkazishi mumkin. Ijtimoiy tarmoq foydalanuvchilari obro'siga qanday ta'sir qilishi mumkinligini ko'rsatadigan bir qator hodisalar mavjud. Misol uchun, 2013-yil dekabr oyida Lacoste xodimi o'z maoshini Instagramda joylashtirgani uchun ishdan bo'shatildi.

Ushbu yangilangan ma'lumotlar ijtimoiy tarmoq xavfsizlik choralari yo'qligi sababli dushmanlar tomonidan ishlatilishi mumkin. Bundan tashqari, foydalanuvchilar ijtimoiy tarmoq profilidagi noto'g'ri ma'lumotlar tufayli ish imkoniyatlarini yo'qotishi mumkin. CareerBuilder tomonidan olib borilgan so'nggi tadqiqotga ko'ra, ishga yollovchilarning 60 foizi kerakli nomzodlar yoki xodimlarni tadqiq qilish uchun ijtimoiy tarmoqdan foydalanadilar. Ijtimoiy tarmoq nafaqat foydalanuvchilarning holati va ishonchliligiga ta'sir qiladi, balki ba'zan ular uchun katta muammolarni keltirib chiqarishi mumkin.

Ijtimoiy tarmoqdagi xavfsizlik tahdidlari. Hozirgi kunda butun dunyo bo'ylab ijtimoiy tarmoqlardan foydalanish jadal sur'atlar bilan o'sib bormoqda. Facebook, Flickr kabi ijtimoiy tarmoqlar milliardlab foydalanuvchilarga shaxsiy ma'lumotlari va multimedia ma'lumotlarini do'stlari, qarindoshlari va boshqa onlayn foydalanuvchilari bilan bo'lishish imkonini beradi.



1.2-rasm. Ijtimoiy tarmoq xavfsizlik tahdidlarining tasnifi.

Multimedia kontentiga tahdidlar - Ma'lumot almashish ijtimoiy tarmoqlarning muhim xususiyati bo'lib, u yerda foydalanuvchilar o'zlarining fotosuratlari, videolari, faoliyati, qiziqishlari va boshqalarni baham ko'rishlari mumkin. Ushbu turdagi ma'lumotlarni almashishning muhim tarkibiy qismlaridan biri multimedia ma'lumotlaridir. Zamonaviy ijtimoiy tarmoq o'z foydalanuvchilariga yuqori aniqlikdagi video va tasvirlarni almashish imkonini beradi. Biroq, joylashuvni taxmin qilish, yuzni aniqlash, veb-qidiruvlar va geotagging kabi multimedia qidiruv usullarining rivojlanishi ushbu elementlardan noqonuniy foydalanish ehtimolini oshirdi. Misol uchun, umumiy rasm geotaggingdan foydalanish orqali foydalanuvchining joylashuvini ko'rsatishi mumkin.

Multimedia kontentini manipulyatsiya qilish – Ijtimoiy tarmoq o'z foydalanuvchilariga juda ko'p multimedia ma'lumotlarini almashishi mumkin bo'lgan platformani taqdim etadi va bu ma'lumotlar ishonchli bo'lmagan foydalanuvchilar tomonidan moslashuvchan va buzib ko'rsatilishi mumkin [9]. Hozirgi vaqtda multimedia ma'lumotlarini buzish uchun bir qancha vositalar mavjud. Ushbu vositalardan foydalangan holda, zararli foydalanuvchi qonuniy foydalanuvchilarning shaxsiy rasmlarini ularga zarar yetkazish yoki masxara qilish uchun buzishi mumkin.

Metadata - Bu boshqa ma'lumotlar haqida ma'lumotni o'z ichiga olgan va yetkazib beradigan ma'lumotlar turi. Ijtimoiy tarmoqlarda multimedia tarkibi metadata vazifasini bajaradi, chunki bu tarkiblar identifikatorlar va joylashuv kabi juda ko'p boshqa qimmatli ma'lumotlarni o'z ichiga oladi. Bu foydalanuvchi uchun qimmatli bo'lsa-da, agar u oshkor etilsa, foydalanuvchi hujumlarga duchor bo'lishi mumkin. Foydalanuvchilarni aniqlashi mumkin bo'lgan multimedia metama'lumotlarining bir turi geo-joy teglaridir. Eng so'nggi mobil telefonlarning bir nechta bosilgan rasmlarga GPS (Global Positioning System) koordinatalarini kiritadi, ular foydalanuvchining joylashuv ma'lumotlarini ochib beradi. Ko'p hollarda rasm metama'lumotlari rasm egasi va ular foydalangan kamera haqidagi ma'lumotlarni oshkor qilishi mumkin. Har bir ijtimoiy tarmoq multimedia metama'lumotlarini boshqacha tarzda boshqaradi. Masalan, Facebook rasmni yuklashdan oldin barcha metama'lumotlarni o'chirib tashlaydi, Google+ esa GPS koordinatalaridan tashqari barcha metama'lumotlarni saqlab qoladi. Flickr xuddi shu joydagi boshqa foydalanuvchilarning rasmlarini ko'rsatish uchun sukut bo'yicha tasvirdagi GPS koordinatalarini ulashadi.

XULOSA

Xulosa qilib aytganda, ijtimoiy tarmoqlar zamonaviy jamiyat hayotining ajralmas qismiga aylangan. Ular insonlar o'rtasidagi muloqotni tezlashtiradi, axborot almashishni osonlashtiradi va global miqyosda ulanish imkonini beradi. Shu bilan birga, ijtimoiy tarmoqlardan noto'g'ri foydalanish ma'naviy, axborotiy va psixologik

muammolarni keltirib chiqarishi mumkin. Ayniqsa, yoshlar orasida vaqtni behuda sarflash, asossiz fikr bildirish va yolg'on axborot tarqatish holatlari uchramoqda.

Shu sababli ijtimoiy tarmoqlardan foydalanishda axborot madaniyatini oshirish, tanqidiy fikrlashni rivojlantirish va shaxsiy ma'lumotlarni himoya qilish muhim ahamiyat kasb etadi. Ijtimoiy tarmoq tahlili esa jamiyatdagi munosabatlar va axborot oqimini chuqur o'rganish imkonini beruvchi samarali ilmiy yo'nalish hisoblanadi.

ADABIYOTLAR RO'YXATI:

1. Castells, M. The Rise of the Network Society. Oxford: Blackwell Publishers, 2010.
2. Boyd, D., Ellison, N. Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 2007.
3. Wasserman, S., Faust, K. Social Network Analysis: Methods and Applications. Cambridge University Press, 1994.
4. Kaplan, A.M., Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 2010.
5. O'zbekiston Respublikasi "Axborotlashtirish to'g'risida"gi Qonuni.
6. O'zbekiston Respublikasi "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi Qonuni.