URGENCH BRANCH OF TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES NAMED AFTER MUHAMMAD AL-KHARIZMI

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

COLLECTION
of materials on topic:

«INFORMATION TECHNOLOGIES, NETWORKS TELECOMMUNICATIONS-ITN&T.2023»

URGENCH - 2023

IJTIMOIY TARMOQLAR VA ULARDAN FOYDALANISHDA XAVFSIZLIK MUAMMOLARI

B. Yu. Palvanov
TATU Urganch filiali kafedra mudiri

Z. B. Yusupova
Xiva prezident maktabi o‘quvchi

I. SH. Nafasov
Urganch davlat universiteti kattao‘qituvchi

K.R. Babadjanov
Urganch davlat universiteti kattao‘qituvchi

Annotation. This article provides evidence-based information on the most common social media scams and how to prevent them.
Keywords. Phishing, Cyberbilling, Ddos attack, information security

Аннотация. В данной статье представлена научно обоснованная информация о наиболее распространенных мошенничествах при использовании социальных сетей и их предотвращении.
Ключевые слова. Фишинг, Кибербиллинг, Ddos атака, информационная безопасность.

Ijtimoiy tarmoqlar bugungi kunda eng mashhur va keng qo'llaniladigan onlayn xizmatlardan biri bo’lib kelmoqda. Ijtimoiy tarmoqlarning ommabopligiga qaramay, ular foydalanuvchi ma'lumotlarini qayta ishlash va saqlash bilan bog'liq ko'plab xavfsizlik muammolari bilan eng zaif kiberolam tizimlardan biri hisoblanadi.

Ijtimoiy tarmoqlar xavfsizligini tashvishga soladigan asosiy masalalardan biri foydalanuvchilarning shaxsiy ma’lumotlarini himoya qilishdir. Ko'pgina foydalanuvchilar ijtimoiy tarmoqlarda o'zlari haqida qancha ma'lumot oshkor qilishlarini tushunmaydilar, bu esa shaxsiy ma'lumotlarning sizib chiqishi va noto'g'ri ishlatilishiga olib kelishi mumkin. Misol uchun, tajovuzkorlar foydalanuvchilarning shaxsiy ma'lumotlaridan firibgarlik, shaxsga oid ma’lumotlarni o'g'irlash va boshqa jinoyatlar uchun foydalanishi mumkin.

Xavfsizlikning yana bir muammosi - bu fishing - foydalanuvchining akaunt ma'lumotlarini ushlash orqali uning hisobiga kirishga urinish. Bu elektron pochta, ijtimoiy media xabarlari, soxta veb-saytlar va boshqa vositalar orqali sodir bo'lishi mumkin. Buzg'unchilar foydalanuvchining akauntiga kirish va shaxsiy ma'lumotlarini o'g'irlash uchun fishingdan foydalanishi mumkin.

Fishing. Ijtimoiy tarmoqlar ham zararli dasturlar va viruslar tarqaladigan joyga aylandi. Bu fishing, tasdiqlanmagan ilovalar, virusli veb-saytlarga havolalar va boshqa vositalar orqali sodir bo'lishi mumkin. Zararli dasturiy ta'minot ma'lumotlarning o'g'irlanishiga, shaxsiy ma'lumotlarning yo'q qilinishiga va qurilmaning ishlamay qolishiga olib kelishi mumkin [1].

Kiberbilling. Ijtimoiy tarmoqlar xavfsizligining eng mashhur muammolaridan biri bu kiberbullingdir. Bu Internetda sodir bo'ladigan va jabrlanuvchi uchun jiddiy psixologik muammolarga olib kelishi mumkin bo'lgan bezorilik, zo'ravonlik va kamsitish jarayonidir. Kiberbulling xabarlar, sharhlar, fotosuratlar va boshqa vositalar orqali sodir bo'lishi mumkin va uning namoyon bo'lishi juda boshqacha bo'lishi mumkin.

***DDos hujum*.** Bundan tashqari, ijtimoiy tarmoqlar kiberhujumlarni tashkil qilish joyiga aylanishi mumkin. Misol uchun, tajovuzkorlar boshqa foydalanuvchilarga, tashkilotlarga yoki hatto ijtimoiy tarmoqning o'ziga hujum qilish uchun ijtimoiy tarmoqlardan foydalanishlari mumkin. Masalan, bu DDoS hujumi bo'lishi mumkin, bu ijtimoiy tarmoq serverlarini ortiqcha yuklashga qaratilgan va uning mavjud bo'lmasligiga olib keladi.

Nihoyat, ijtimoiy tarmoqlar ham noto'g'ri ma'lumotlar va soxta xabarlar tarqaladigan joyga aylandi. Bu jiddiy ijtimoiy oqibatlarga olib kelishi mumkin, masalan, ijtimoiy barqarorlikning buzilishi, siyosiy inqirozlar va boshqalar.

Xavfsizlikni ta’minlashning dastlabki choralari. Ushbu muammolarni hal qilish uchun ijtimoiy tarmoqlar xavfsizligini ta'minlash bo'yicha kompleks chora-tadbirlarni amalga oshirish kerak. Foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish usullarini takomillashtirish, foydalanuvchilarni ijtimoiy tarmoqlardan xavfsiz foydalanish bo'yicha muntazam ravishda o'rgatish va jinoyat sodir etilgan taqdirda huquqni muhofaza qilish organlariga murojaat qilish muhim ahamiyatga ega[2].

Shuningdek, ijtimoiy tarmoqlarni himoya qilishning texnik vositalarini takomillashtirish, masalan, ma'lumotlarni shifrlash, fishing va viruslardan himoya qilish, shuningdek, zararli giperhavolalarni aniqlash va blokirovka qilish algoritmlarini takomillashtirish zarur.

Umuman olganda, ijtimoiy tarmoqlar xavfsizligi foydalanuvchilar, ijtimoiy tarmoqlarga ega bo‘lgan kompaniyalar va davlat organlarining o‘zaro hamkorligini talab qiluvchi murakkab vazifadir. Faqat birgalikda ishlash orqali biz onlayn muhitda xavfsizlikni ta'minlashimiz va foydalanuvchilar va butun jamiyat uchun jiddiy oqibatlarning oldini olishimiz mumkin.

Ijtimoiy tarmoqlardagi yana bir xavfsizlik muammosi mualliflik huquqining buzilishidir. Foydalanuvchilar boshqa odamlarning intellektual mulki bo'lgan fotosuratlar, videolar va musiqa kabi kontentni yuklashlari mumkin. Bu esa foydalanuvchilar uchun sud jarayonlari va jarimalar, shuningdek, ijtimoiy tarmoq obro‘siga putur yetkazishi mumkin.

Bundan tashqari, ijtimoiy tarmoqlar kiberbulling va onlayn zo'ravonlikning boshqa shakllari uchun maydonga aylanishi mumkin. Foydalanuvchilarni masxara qilish, kamsitish va haqorat qilish mumkin, bu esa jiddiy psixologik oqibatlarga olib kelishi mumkin. Ba'zi foydalanuvchilar hatto o'z joniga qasd qilishga urinishlari mumkin. Ijtimoiy tarmoqlar zo'ravonlik va ekstremizmni tarqatish uchun ham ishlatilishi mumkin. Hujumchilar ijtimoiy tarmoqlardan tashviqot olib borish va o'z tashkilotlariga yangi a'zolarni jalb qilish uchun foydalanishlari mumkin. Bu jamiyat xavfsizligi uchun jiddiy oqibatlarga olib kelishi mumkin.

Umuman olganda, ijtimoiy tarmoqlar xavfsizligi bilan bog'liq muammolar jiddiy bo'lib, foydalanuvchilar va butun jamiyat uchun jiddiy oqibatlarga olib kelishi mumkin. Ushbu muammolarni hal qilish uchun ijtimoiy tarmoqlar xavfsizligini ta’minlash, jumladan, texnik himoya vositalarini takomillashtirish, foydalanuvchilarni ijtimoiy tarmoqlardan xavfsiz foydalanishga o‘rgatish, huquqni muhofaza qiluvchi organlar bilan o‘zaro hamkorlik qilish bo‘yicha kompleks chora-tadbirlarni amalga oshirish zarur.

Qarshi kurashish usullari.

Axborotni himoya qilish uchun qo'llanilishi mumkin bo'lgan umumiy xavfsizlik choralarini ko'rish bo'lib, ular quyidagilardan iborat:

Autentifikatsiya va avtorizatsiya: Parollar, biometrikalar yoki smart-kartalar kabi autentifikatsiya usullaridan foydalangan holda faqat vakolatli foydalanuvchilar maxfiy ma'lumotlarga kirishiga ishonch hosil qilish va ma'lum ma'lumotlarga kirishga ruxsat berish yoki rad etish uchun avtorizatsiya tizimini o'rnatish.

Ma'lumotlarni shifrlash: tarmoq orqali ma'lumotlar o'tayotganda yoki qurilmalarda saqlangan maxfiy ma'lumotlarni himoya qilish uchun kriptografik algoritmlardan foydalanish. Masalan, ***SSL*** yoki ***TLS*** shifrlash Internet orqali uzatiladigan ma'lumotlarni himoya qilishi mumkin.

Xavfsizlik auditi: Ruxsatsiz kirish urinishlarini kuzatish va xavfsizlik siyosatlariga rioya etilishini ta'minlash uchun maxfiy ma'lumotlar bilan barcha harakatlarni yozib olish.

Dasturiy ta'minotni yangilash: zarur ma'lumotlarni qayta ishlash va saqlash uchun foydalaniladigan barcha dasturiy ta'minot zaifliklarni bartaraf etish va xavfsizlikni ta'minlash uchun muntazam ravishda yangilanib turishini ta'minlash.

Fizik xavfsizlik: Signalizatsiya va boshqa tizimlari kabi kirishni boshqarish mexanizmlari yordamida qurilmalar va ma'lumotlarni saqlashning jismoniy xavfsizligini ta'minlash.

O'qitish va o'rgatish: Foydalanuvchilarni xavfsizlik amaliyotlari, shu jumladan ma'lumotlarning maxfiyligini saqlash zarurati va xavfsiz ma'lumotlarni saqlash va qayta ishlash usullaridan foydalanish zaruriyatiga o'rgatish.

Hulosa. Umuman olganda, yuqorida keltirilgan choralar ijtimoiy tarmoqlarda foydalanish xavfsizligini yaxshilashda muhim qadamdir, lekin u barcha xavfsizlik masalalari uchun mukammal yechim emas va boshqa xavfsizlik choralari bilan birgalikda ko'rib chiqilishi kerak.

Foydalanilgan adabiyotlar

1. Ковалёв Сергей Сергеевич, and Шишаев Максим Геннадьевич. "Современные методы защиты от нежелательных почтовых рассылок" Труды Кольского научного центра РАН, no. 7, 2011, pp. 100-111.
2. Мироненко А. Н. Метод распознавания спам-сообщений на основе анализа заголовка письма // МСиМ. 2010. №1 (21).