BUGUNGI KUNDAGI KIBER TAHDIDLAR VA ULARDAN HIMOYALANISH

Muyitdinov Elbek Ruyitdinovich
Халкаро инновацион университет "Иктисодиёт ва молия" кафедра мудири
elbek.muyitdinov@gmail.com
https://doi.org/10.5281/zenodo.15099399

Annotatsiya

Texnologiyalar rivoji bilan bir qatorda kiberxavfsizlik masalasi bugungi kunda dolzarb muammolardan biriga aylandi. Internetdan foydalanish darajasi ortib borayotgan O‘zbekiston ham bundan mustasno emas. Ushbu maqolada zamonaviy kiberhujumlar, ularning iqtisodiy zarari va ulardan himoyalanish usullari haqida so‘z yuritamiz.

Kalit so‘zlar: kiberhujum turlari, bank kartalari xavfsizligiga tahdidlar, mobil ilovalar, zararli dasturlar, telefon orqali firibgarlik, Wi-Fi orqali hujumlar, troyan dasturlari, antivirus va xavfsizlik dasturlari va xodimlarni o‘qitish.

Аннотация

С развитием технологий проблема кибербезопасности стала одной из актуальных проблем сегодня. Узбекистан, где растет использование интернета, не является исключением. В этой статье мы поговорим о современных кибератаках, их экономическом ущербе и способах защиты от них.

Ключевые слова: типы кибератак, угрозы безопасности банковских карт, мобильные приложения, вредоносные программы, телефонное мошенничество, атаки через Wi-Fi, трояны, антивирусное программное обеспечение и программное обеспечение безопасности, а также обучение сотрудников.

Annotation

Along with the development of technologies, the issue of cyber security has become one of the pressing problems today. Uzbekistan, which is growing in the level of internet use, is no exception. In this article, we will talk about modern cyber attacks, their economic harm and methods of protection against them.

Keywords: types of cyberattacks, threats to bank card security, mobile applications, malware, phone fraud, Wi-Fi attacks, Trojan programs, antivirus and security programs, and employee training.

Kiberhujum turlari

Kiberxavfsizlik sohasidagi muammolar ko‘pincha quyidagi hujum turlarida namoyon bo‘ladi:

1. **Fishing (fişing):** Hujumchilarning eng keng tarqalgan usullaridan biri bo‘lib, ular foydalanuvchini aldash orqali maxfiy ma’lumotlarni (parollar, kredit karta ma’lumotlari) qo‘lga kiritadi. Odatda, bu hujumlar elektron pochta yoki ijtimoiy tarmoqlar orqali amalga oshiriladi. Xususan, O‘zbekistonda soxta onlayn savdo platformalari orqali ham fişing hujumlari kuzatilmoqda.
2. **Ransomware (shantaj dasturlari):** Ushbu dasturlar orqali kiberjinoyatchilar tizimdagi ma’lumotlarni bloklab qo‘yadi va ochish uchun katta miqdorda pul talab qiladi. 2020-yilning o‘zida ransomware hujumlari global miqyosda milliardlab dollarlik zarar yetkazgan. O‘zbekistonning kichik va o‘rta korxonalari ham bu turdagi hujumlarga duch kelmoqda.
3. **DDoS hujumlari:** Bunday hujumlar orqali jinoyatchilar sayt yoki tizimning ishlashini to‘xtatib qo‘yish uchun ularni ortiqcha ma’lumot oqimi bilan to‘ldiradi. DDoS hujumlari, ayniqsa, davlat xizmatlari yoki bank tizimlari faoliyatiga putur yetkazishi mumkin.
4. **Zararli dasturlar:** Kompyuter viruslari, troyanlar va boshqa zararli kodlar orqali hujumlar uyushtiriladi. Ular tizimni buzish, ma’lumotlarni o‘g‘irlash yoki foydalanuvchi faoliyatini kuzatish uchun ishlatiladi. Mobil ilovalar orqali zararli dasturlar tarqalishi ham dolzarb muammolardan biridir.
5. **Tarmoq orqali buzib kirish:** Hujumchilar zaif parollar yoki xavfsizlikning past darajasidan foydalanib tarmoqqa noqonuniy kirishadi. Masalan, Wi-Fi tarmoqlarida zaif shifrlash protokollari hujumchilarga imkoniyat yaratadi.

Fuqarolarning bank kartalari xavfsizligiga tahdidlar

Bank kartalaridan pulni noqonuniy ravishda yechib olish kiberjinoyatchilikning keng tarqalgan usullaridan biridir. Quyida bu borada qo‘llaniladigan asosiy usullar va ulardan himoyalanish yo‘llari keltiriladi:

1. **Soxta saytlar orqali ma’lumotlarni o‘g‘irlash:** Jinoyatchilar asliga o‘xshash soxta bank saytlarini yaratib, foydalanuvchilardan karta ma’lumotlarini kiritishni so‘raydi. Bu usulda, ko‘pincha, reklama bannerlari yoki spam xabarlari orqali saytga o‘tish taklif qilinadi.
   - **Himoya chorasi:** Rasmiy bank saytlariga faqat ishonchli havolalar orqali kiring. HTTPS protokoli va yashil qulf belgisining mavjudligini tekshiring.
2. **Mobil ilovalar orqali zararli dasturlar:** Soxta banking yoki to‘lov ilovalari foydalanuvchilarni aldab karta ma’lumotlarini kiritishga undaydi yoki qurilma orqali to‘lov ma’lumotlarini o‘g‘irlaydi.

- **Himoya chorasi:** Mobil ilovalarni faqat rasmiy do‘konlardan (Google Play, App Store) yuklab oling va ilova reytinglari hamda sharhlarini tekshiring.

3. **ATM skimming (skimming qurilmalari):** Jinoyatchilar bankomatlarga maxsus qurilmalar o‘rnatib, karta ma’lumotlarini nusxalaydi va keyinchalik ushbu ma’lumotlardan foydalanib mablag‘ni o‘zlashtiradi.

- **Himoya chorasi:** Bankomatda shubhali narsalar borligini tekshiring. Kartani kiritish joyida bo‘shliq yoki g‘alati qurilmalar mavjudligini ko‘zdan kechiring.

4. **Telefon orqali firibgarlik:** Hujumchilar o‘zlarini bank xodimi sifatida tanishtirib, karta ma’lumotlarini so‘raydi. Bu ma’lumotlarni olish orqali ular hisobdan mablag‘ni o‘zlashtiradi.

- **Himoya chorasi:** Bank xodimlari hech qachon telefon orqali karta ma’lumotlarini so‘ramasligini yodda saqlang. Shubhali qo‘ng‘iroqlar haqida darhol bankka xabar bering.

5. **Ommaviy Wi-Fi orqali hujumlar:** Ochiq Wi-Fi tarmoqlarida jinoyatchilar foydalanuvchi qurilmalariga kirib, karta ma’lumotlarini kuzatishi mumkin.

- **Himoya chorasi:** Ommaviy tarmoqlarda tranzaksiyalarni amalga oshirmang va VPN xizmatlaridan foydalaning.

6. **Troyan dasturlari:** Elektron pochta yoki zararli havolalar orqali foydalanuvchi qurilmasiga troyan dasturlar o‘rnatiladi va ular karta ma’lumotlarini kuzatib boradi.

- **Himoya chorasi:** Elektron pochta orqali kelgan noma‘lum xabarlarni ochmang va antivirus dasturlarini muntazam yangilang.

Kiberhujumlarning iqtisodiy zarari

Kiberjinoyatchilik nafaqat ma’lumotlar xavfsizligiga, balki iqtisodiyotga ham katta zarar yetkazadi. Jahon miqyosida, 2025-yilga kelib, kiberjinoyatlar tufayli yetkazilgan iqtisodiy zarar 10,5 trillion AQSh dollariga yetishi prognoz qilinmoqda. O‘zbekiston sharoitida ham bu muammo sezilarli darajada. Quyidagi omillar iqtisodiy zararlarni keltirib chiqaradi:

- **Moliyaviy yo‘qotishlar:** Bank hisoblaridan noqonuniy pul yechib olish yoki shantaj natijasida katta mablag‘ yo‘qoladi. Masalan, soxta banking ilovalari orqali firibgarlik holatlari ortib bormoqda.
- **Ishlab chiqarishning to‘xtashi:** Tizimlarning buzilishi korxonalarning faoliyatini vaqtincha to‘xtatadi, bu esa daromadning kamayishiga olib keladi. Bir necha soatlik uzilishlar ham korxonalar uchun katta zarar keltirishi mumkin.

- **Obro‘ga putur yetishi:** Ma’lumotlar sizib chiqishi kompaniya yoki tashkilotning nufuziga zarar yetkazadi. Bu mijozlar ishonchini yo‘qotishga olib keladi.
- **Qo‘shimcha xarajatlar:** Tizimni qayta tiklash, mutaxassislarni jalb qilish va yangi xavfsizlik choralarini amalga oshirish qo‘shimcha mablag‘ talab qiladi.

Kiberxavfsizlik bo‘yicha himoya choralar

Kiberhujumlardan samarali himoyalanish uchun quyidagi choralar tavsiya etiladi:

1. **Kuchli parollar yaratish:** Oddiy va oson topiladigan parollardan foydalanmaslik kerak. Parollar murakkab va uzoqroq bo‘lishi, harflar, raqamlar va belgilarni o‘z ichiga olishi lozim. Shuningdek, har bir xizmat uchun alohida parol ishlatish tavsiya etiladi.
2. **Antivirus va xavfsizlik dasturlaridan foydalanish:** Tizimlarni zararli dasturlar va hujumlardan himoya qilish uchun doimo yangilanib turuvchi antivirus dasturlaridan foydalaning.
3. **Ikki faktorli autentifikatsiya:** Muayyan xizmatlarga kirishda ikki bosqichli tekshiruvni yoqing. Bu usul kiberjinoyatchilarning hisobingizga kirishini sezilarli darajada qiyinlashtiradi.
4. **Tarmoq xavfsizligini ta’minlash:** Wi-Fi tarmoqlarini kuchli parol va shifrlash protokollari bilan himoya qiling. Ochiq tarmoqlarda faqat ishonchli VPN xizmatlaridan foydalaning.
5. **Muntazam ravishda zaxira nusxalar yaratish:** Muhim ma’lumotlarni tashqi qurilma yoki bulut xizmatlariga saqlang. Shunday qilib, ransomware kabi hujumlarda ma’lumotlaringizni qayta tiklash imkoniyati bo‘ladi.
6. **Xodimlarni o‘qitish:** Tashkilotlarda xodimlarga kiberxavfsizlik bo‘yicha muntazam treninglar o‘tkazing. Ko‘pchilik kiberhujumlar inson omiliga bog‘liq bo‘lgan xatolar tufayli amalga oshadi.
7. **Shubhali xabarlarni ochmaslik:** Elektron pochta orqali kelgan noma’lum havolalar yoki fayllarni ochishdan oldin ularning ishonchliligini tekshiring.
8. **Maxsus dasturlar va xizmatlardan foydalanish:** Bank operatsiyalarida rasmiy banking ilovalaridan foydalaning va tranzaksiyalarni faqat ishonchli qurilmalardan amalga oshiring.

Xulosa

Bugungi kunda kiberxavfsizlik muammolari nafaqat texnologik rivojlanish, balki iqtisodiy va ijtimoiy barqarorlikka ham ta’sir ko‘rsatmoqda. O‘zbekiston

fuqarolari va tashkilotlari kiberxavfsizlik choralariga jiddiy yondashishi zarur. Kuchli parollar, xavfsiz tarmoqlar, antivirus dasturlar va xodimlarni o‘qitish orqali biz ushbu tahdidlarni kamaytirishimiz va raqamli muhitda xavfsizlikni ta’minlashimiz mumkin.

Adabiyotlar:

1. Stuttard, D., & Pinto, M. (2011). The web application hacker's handbook: Finding and exploiting security flaws. John Wiley & Sons.
2. Erickson, J. (2008). Hacking: the art of exploitation. No starch press.
3. Singer, P. W., & Friedman, A. (2013). Cybersecurity and Cyberwar: What Everyone Needs to Know®. Oxford University Press.
4. Sikorski, M., & Honig, A. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press.
5. Ch H. Social Engineering: The Science of Human Hacking. – 2014.
6. Stallings, W., & Brown, L. (2015). Computer security: principles and practice. Pearson.
7. Weidman, G. (2014). Penetration testing: a hands-on introduction to hacking. No starch press.
8. Bozarov, D. (2023). Bo ‘lajak iqtisodchi talabalarning iqtisodiy kompetensiyasini rivojlantirishning matematik tahlili. Академические исследования в современной науке, 2(27), 84-90.
9. Allamova, M., & Bozarov, D. (2023). Trigonometrik tengsizliklar yechimlarining innovatsion qo ‘llanilishi. Евразийский журнал математической теории и компьютерных наук, 3(1), 75-78.
10. Bozarov, D. (2022). PROBLEMS OF SYSTEMS OF LINEAR ALGEBRAIC EQUATIONS. Science and Innovation, 1(2), 163-171.