ONLAYN FIRIBGARLIKLAR VA BANK KARTALARIDAGI MABLAG'LARNI HIMOYA QILISH

Akramov Xurshidbek Bahrom o'g'li
Komilov Omadjon Xursandbek o'g'li
Andijon iqtisodiyot va qurilish instituti Iqtisodiyot kafedrasi 3-kurs talabalari

Annotatsiya: *Texnologiya rivojlanishi bilan kiberjinoyatchilar moliyaviy hisoblarni buzish va maxfiy ma'lumotlarni o'g'irlash uchun foydalanadigan usullar ham o'sib bormoqda. Ushbu maqolada bank kartalaringiz xavfsizligini oshirish, jismoniy va raqamli zaifliklarni bartaraf etish bo'yicha batafsil tavsiyalar berilgan. Tavsiya etilgan strategiyalarni amalga oshirish va hushyor bo'lish orqali o'quvchilar firibgarlik, skanerlash qurilmalari va onlayn firibgarlik qurboni bo'lish xavfini kamaytirishi mumkin.*

Annotation: *As technology advances, so do the methods cybercriminals use to breach financial accounts and steal sensitive information. This article provides detailed recommendations on how to increase the security of your bank cards and eliminate physical and digital vulnerabilities. By implementing the recommended strategies and being vigilant, students can reduce their risk of falling victim to scams, scanning devices, and online scams.*

Kalit so'zlar: *kartalari, xavfsizlik, kiber tahdidlar, Skimming qurilmalari, Onlayn tranzaksiyalar, sms xabarnomalar, bankomat*

XXI asr raqamli texnologiyalar asri bo'lib, texnologik taraqqiyot jadallik bilan rivojlanmoqda. Insonlarning shaxsiy hayotida o'zgarishlar amalga oshirib, ularning turli ehtiyojlarini osonlik bilan hal etishda yordam bermoqda. Misol uchun, shunchaki bank plastik kartalari orqali keng ko'lamli moliyaviy operatsiyalarni, ya'ni oylik maosh, pensiya va nafaqa olish, kommunal to'lovlarni hamda kreditlarni masofadan turib amalga oshirish, soliqlar va boshqa turli to'lovlarni osonlikcha amalga oshirishimiz mumkin va bu qulayliklar bank kartalariga bo'lgan talabni oshirmoqda va o'z navbatida moliyaviy tranzaktsiyalar uzluksiz va hamma joyda bo'lib qolgan bugungi o'zaro bog'langan raqamli muhitda bank kartalarimizni himoya qilish har qachongidan ham muhimroqdir. Kibertahdidlar doimiy ravishda rivojlanib borayotgani va firibgarlik sxemalari yanada murakkablashib borayotgan bir sharoitda moliyaviy aktivlarimiz xavfsizligini ta'minlash ustuvor vazifaga aylandi. Jismoniy o'g'irlik, skanerlash qurilmalari yoki onlayn firibgarlikdan himoya qilish bo'ladimi, bu yerda keltirilgan tavsiyalar odamlarga o'z moliyaviy hisoblarining yaxlitligini saqlash uchun faol choralar ko'rish imkonini beradi. Xatarlarni tushunish va samarali qarshi choralarni qo'llash orqali o'quvchilar o'zlarining pullari ruxsatsiz kirish va firibgarlik faoliyatidan himoyalanganligini bilib, raqamli moliyaviy muhitda ishonch bilan harakat qilishlari mumkin.

Avval, "firibgarlik" tushunchasiga to'xtalib o'tamiz, firibgarlik- bu aldash yo'li bilan birovning mulkini egallab olish yo'li bo'lgan har xil turdagi mol-mulkni o'g'irlash ko'rinishini bildiradi va bugungi bu olayn tarzda ham amalga oshirilmoqda. Bunday firibgarlik doirasiga kirib kelgan yangi atama bu "vishing" hisoblanadi, ya'ni foydalanuvchi, masalan, bank xodimidan telefon qo'ng'irog'ini oladi va operator, agar darhol telefon orqali to'liq ma'lumot

berilmasa, uning bank kartasi, shu jumladan uning raqami, CVV-kodi va boshqalar bloklanishi haqida ogohlantiradi, mijoz vahima boshlaydi va barcha shaxsiy ma'lumotlarni beradi va pul mablag’rini yoqotadi. Yana bir jinoiy sxema - Jinoiy sxema foydalanuvchini SMS-xabardagi zararli havolani bosishga qaratilgan. Xabar taniqli bankdan, tanish kompaniyadan bildirishnoma shaklida bo'lishi mumkin yoki to'satdan lotereya yutug'i haqida ma'lumot bo'lishi mumkin va hokazo. Skimming - bu jinoyatchilar tomonidan karta egasidan ma'lumot olish uchun ishlatiladigan usul. Firibgarlar skimmer deb ataladigan kichik qurilma yordamida eng ilg'or yondashuv bilan karta ma'lumotlarini olish uchun bir nechta yondashuvlardan foydalanishlari mumkin. Ushbu jinoiy usul identifikatsiya o'g'rilariga karta egasidan firibgarlik operatsiyalari uchun ishlatilishi mumkin bo'lgan ma'lumotlarni to'plash imkonini beradi. Skimming texnologiyasi yil sayin takomillashib bormoqda, bu esa ushbu turdagi firibgarlikka qarshi kurashishni qiyinlashtiradi.

Bunday firibgarlilarga qarshi kurashish uchun markaziy bank, tijorat banklari hamda karta emitentlari turli choralarni ko’rishi shart hisoblanadi. Jumladan, “O‘zbekiston Respublikasi hududida bank kartalarining chiqarilishi va muomalada bo‘lishi qoidalari to‘g‘risida”gi nizomda quyidagilar belgilab ketilgan: Emitentlar, ekvayerlar, to‘lov tizimi operatorlari, savdo va xizmat ko‘rsatish subyektlari bank kartalari orqali hisob-kitoblarni amalga oshirishda foydalaniladigan axborotlarni va dasturiy-texnik vositalarni himoya qilish bo‘yicha qoidalarga rioya qilishlari shart; Axborotlarni, bank kartalarini va bunda foydalaniladigan dasturiy-texnik vositalarni himoya qilish, O‘zbekiston Respublikasining qonunchiligi hamda to‘lov tizimining qoida va tartiblariga asosan o‘rnatiladi. Shuningdek iste’molchilar uchun ham quyidagi tavsiyalarga amal qilishi muhim hisoblanadi:

1. Kartangizni xavfsiz saqlang: Bank kartalaringizni jismoniy nazorat qilish ularning xavfsizligi uchun asosiy hisoblanadi. Kartalaringizni har doim xavfsiz joyda, masalan, hamyoningizda yoki karta egasi bilan birga saqlang va ularni jamoat joylarida qarovsiz qoldirmang. Kartangiz ma'lumotlarini, jumladan, karta raqamini, amal qilish muddatini va xavfsizlik kodini hech kimga oshkor qilishdan saqlaning. Bundan tashqari, shaxsiy identifikatsiya raqamingizni (PIN) hech qachon boshqalarga oshkor qilmang, uning maxfiyligini ta’minlang.

2. Skimming qurilmalaridan ehtiyot bo'ling: Skimming qurilmalari bank kartalari xavfsizligiga jiddiy tahdid solib, firibgarlarga karta ma'lumotlarini noqonuniy ravishda olish imkonini beradi. Avtomatlashtirilgan bankomatlar (bankomatlar) yoki kartani o'qish moslamalaridan foydalanganda ehtiyot bo'ling va bu qurilmalarda o'zgartirish belgilari yoki shubhali biriktirmalarni diqqat bilan tekshiring. Bankomat yoki savdo nuqtasi terminalida PIN-kodni kiritayotganda, kuzatuvning oldini olish uchun klaviaturani yoping. Iloji bo'lsa, yaxshi yoritilgan va aholi zich joylashgan joylarda joylashgan bankomatlarni tanlang, chunki ular xakerlik va firibgarlikka kamroq moyil.

3. Xavfsiz onlayn tranzaktsiyalardan foydalaning: Onlayn tranzaktsiyalar keng tarqalgan bo'lib, raqamli tijorat bilan bog'liq xavflarni kamaytirish uchun xavfsiz amaliyotlarni amalga oshirish juda muhimdir. Onlayn xaridlar uchun ishonchli veb-saytlar va ishonchli to‘lov usullaridan foydalanishga ustuvor ahamiyat bering, ular maxfiy ma’lumotlaringizni himoya qilish uchun kuchli shifrlash protokollaridan foydalanishiga ishonch hosil qiling.

Himoyalanmagan yoki ommaviy Wi-Fi tarmoqlari orqali moliyaviy operatsiyalarni amalga oshirishdan saqlaning, chunki ular jinoyatchilar tomonidan ushlanishi mumkin.

4. Xavfsizlik xususiyatlaridan foydalaning: Ko'pgina banklar va karta emitentlari o'z mijozlarining hisoblari va tranzaksiyalari xavfsizligini oshirish uchun bir qator xavfsizlik xususiyatlari va vositalarini taklif etadilar. Hisobingizdagi har qanday harakat haqida sizni real vaqtda xabardor qiladigan tranzaksiya ogohlantirishlarini yoqish orqali ushbu takliflardan foydalaning. Ruxsatsiz kirishni oldini olish uchun qo'shimcha tasdiqlash qatlamini qo'shib, onlayn xaridlar uchun ikki faktorli autentifikatsiyani (2FA) amalga oshirishni ko'rib chiqing. Iloji bo'lsa, tranzaktsiyalaringiz va hisobingizga kirish xavfsizligini oshirish uchun barmoq izlari yoki yuzni tanish kabi biometrik autentifikatsiya usullaridan foydalaning.

Bundan tashqari, bank kartalaringiz uchun sarf-xarajatlar yoki tranzaksiya cheklovlarini o'rnatishni ko'rib chiqing. Ushbu sozlanishi mumkin bo'lgan xususiyatlar sizga kartangizdan foydalanishni yanada samarali nazorat qilish va nazorat qilish imkonini beradi, soxta tranzaksiyalar yoki ruxsatsiz xaridlarning mumkin bo'lgan ta'sirini cheklaydi.

Xulosa qilganda, bank kartangizdagi pullarni himoya qilish tirishqoqlik, xabardorlik va potentsial xavflarni kamaytirish uchun faol choralarni talab qiladi. Ushbu maqolada keltirilgan maslahatlarga amal qilish va paydo bo'ladigan tahdidlarga qarshi hushyor bo'lish orqali siz firibgarlik yoki ruxsatsiz tranzaktsiyalar qurboni bo'lish ehtimolini sezilarli darajada kamaytirishingiz mumkin. Esingizda bo'lsin, moliyaviy aktivlaringizni himoya qilish doimiy mas'uliyatdir, u doimo o'zgarib turadigan kiber tahdidlar dunyosida e'tibor va hushyorlikni talab qiladi. Xabardor bo'ling, faol bo'ling va moliyaviy farovonligingizni ishonchli himoya qiling.

FOYDALANILGAN ADABIYOTLAR:

1. Зыков ДюАю Виктимологические аспекты предупреждения компьютерного мошенничества. 2002 г.
2. “O‘zbekiston Respublikasi hududida bank kartalarining chiqarilishi va muomalada bo‘lishi qoidalari to‘g‘risida”gi nizom, 03.04.2021
3. https://finlit.uz/uz/articles/payments-and-transfers/protect-money-on-the-card/
4. https://ipakyulibank.uz/physical/kartalar/help/kartalarni-xavfsiz-ishlatish-qoidalari