Plastik kartadan pulingiz o‘g‘irlanmasligi uchun nima qilish kerak? Amaliy tavsiyalar

Tursunboyeva Dinora Islom qizi
Toshkent davlat yuridik universiteti talabasi

Abstrakt

Maqolada O‘zbekistonda plastik kartalarning ahamiyati qo'llanilishi va qulayliklari haqida ma'lumot berilgan. Plastik kartadagi pullarning xavfsizlik darajasi turli tomondan o'rganilgan. Va eng muhimi kartadan pul o'g'irlanmasligi uchun kerakli amaliy tavsiyalar berib o‘tilgan..

Kalit so‘zlar: Plastik karta, bankomat, xavf, chegirma, Vizitkalar, raqamlash tizimi, emitent identifikatorlar.

Kirish

Plastik kartalar bugungi kunda moliyaviy operatsiyalarda keng qo'llaniladi. Ular debet kartalari, kredit kartalari va bankomat kartalari kabi turli shakllarda bo'lishi mumkin. Plastik kartalar naqd pulni olib yurish zaruratini kamaytiradigan xavfsiz va oson to‘lov usulini taklif etadi. Ular, shuningdek, atrof-muhitga kamroq zarar etkazadigan alternativ sifatida ajralib turadi.

Plastik karta - bu mexanik va termal ta'sirlarga chidamli bo'lgan maxsus plastmassadan tayyorlangan standart o'lchamdagi plastinkadir (ko'pincha 54 × 86 × 0,76 mm). Kartochkalar maqsadi, funktsional va texnik xususiyatlari bilan farqlanadi.

Plastik kartalar ishlatilishi (bitta karta uchun bir nechta ilovalar mavjud):

-ularning egasini aniqlash;

-to'lov vositalarining analogi sifatida;

-sodiqlik dasturlarida ishtirok etish imkonini beradi (mini-kartalar / kalitlar, sovg'a, chegirma, reklama / klub, chiptalar / sertifikatlar, tayyor mahsulotlar uchun sifat sertifikatlari, kontaktsiz kartalar va boshqalar);

Ushbu kartalar plastik kartochkalarning jismoniy xususiyatlaridan tortib kartaning o'lchamiga qadar va u yoki bu tarzda kartada joylashtirilgan ma'lumotlarning

mazmuniga qadar plastik kartalarning deyarli barcha xususiyatlarini belgilaydigan standartlar bilan birlashtirilgan:

-ISO-7810 "Identifikatsiya kartalari - jismoniy xususiyatlar";

-ISO-7811 "Identifikatsiya kartalari - qayd etish usullari";

-ISO-7812 “Identifikatsiya kartalari – raqamlash tizimi va emitent identifikatorlarini ro‘yxatdan o‘tkazish tartibi” (5 qism);

-ISO-7813 "Identifikatsiya kartalari - moliyaviy operatsiyalar uchun kartalar";

-ISO-4909 "Bank kartalari - magnit chiziqning uchinchi treki tarkibi";

-ISO-7816 "Identifikatsiya kartalari - kontaktli mikrochip kartalari" (6 qism).

Maqsadlari bo'yicha plastik kartochkalar turlari identifikatsiya kartalari :

-pasportlar, haydovchilik guvohnomalari, avtomashinalarni ro'yxatdan o'tkazish

ijtimoiy kartalar (masalan, Moskvadagi talabaning ijtimoiy kartasi)

shaxsiy guvohnomalar (turli odamlar guruhlari uchun, masalan, saylovchilar, kambag'allar va boshqalar) P.)

-ovoz berish uchun deputatlarning kartochkalari

Vizitkalar sodiqlik plastik kartalari (sodiqlik dasturining turiga qarab tayinlanadi): chegirma kartalari, sovg'a sertifikatlari, klub kartalari, jamg'arib boriladigan / bonus - plastik kartalari

-bank to'lov kartalari

-kredit kartalari

-debet kartalari

-bojxona kartalari

-aloqa kartalari

SIM-kartalar (faqat dastlabki SIM-kartalar ISO 7810 standartiga muvofiq to'liq hajmda ishlab chiqarilgan)

-USIM kartalari

-R-UIM kartalari

-taksofon kartalari

-oldindan to'langan kartalar

-skretch kartalari . Aloqa xizmatlarini to'lash uchun xizmat qiladi.

-tarif kartalari (elektron sayohat kartasi)

-yoqilg'i kartalari

-qo'ng'iroq kartalari (simli, simsiz va IP-telefoniya)

-raqamli televideniyega kirish kartalari

-elektr to'lov kartalari

-to'xtash joyi to'lov kartalari

-kompyuter o'yini uchun faollashtirish kalitlari bilan kartalar

-Mediasiz raqamli kartalar

-shtrix-kod kartalari

-magnit chiziqli kartalar, magnit chiziqda o'nlab baytlarni saqlaydigan kartalar

smart-kartalar - chipli kartalar (taxminan 32 KB o'rnatilgan xotiraga ega mikroprotsessor), ular aloqa usuliga qarab quyidagilarga ajratiladi:

-kontaktsiz kartalar (RFID, masalan, NFC)

-kontakt kartalari (ISO/IEC 7810, ISO/IEC 7816 va boshqalar)

-birlashtirilgan magnit-chipli kartalar, ham chip, ham magnit chiziqni o'z ichiga oladi

Kartalarni shaxsiylashtirish turlari

-shtrix-kod - shtrixlar ko'rinishida kodlangan harf-raqam ma'lumotlarini kartaga chizish;

-Bo'rttirma (shtamplash) - plastik kartochka yuzasiga bo'rttirma belgilar ko'rinishidagi harf-raqamli ma'lumotlarni keyinchalik bo'yash mumkin bo'lgan holda qo'llash. Ma'lumotlarni mexanik nusxa ko'chirish imkoniyatini beradi (masalan, imprinter yordamida). Belgilarni bo'rttirish faqat kartaning gorizontal yo'nalishi bilan mumkin. Bo'rttirma ikki turdagi shriftlarda amalga oshiriladi: 4,5 mm balandlikda - katta (faqat raqamlar); 3 mm balandlikda - kichik (raqamlar va harflar).

-indent bosib chiqarish - bu plastik karta yuzasiga tekis belgilar ko'rinishidagi harf-raqamli ma'lumotlarni keyingi kiritish (bo'yash) bilan qo'llash. Faqat "elektron" foydalanish uchun mo'ljallangan kartalar uchun odatiy;

magnit chiziq - kartaga magnit saqlovchi vositani keyinchalik ma'lumotlarni yozib olish bilan chizish; yozish uchun uchta trekka ega: biri harf-raqamli ma'lumot uchun va ikkita trek raqamlar uchun.

-imzo paneli - karta yuzasiga qo'llaniladigan maxsus qatlam, sizga yozuvlar qo'yish imkonini beradi;

-skretch (scratch)-panel - himoyalangan ma'lumotlar (pin-kod, yutuq so'zi, hisobni to'ldirish kodi va boshqalar) ustidan karta yuzasiga qo'llaniladigan shaffof bo'lmagan himoya qatlami. d.);

-chip - kartaga o'rnatilgan mikroprotsessorga asoslangan axborot tashuvchisi. Yoki prokladkaga ega yoki radio aloqasidan (RFID) foydalanadi.

Kartani himoya qilish turlari

-gologramma

-mikroskript, iz elementlari

-ustiga bosib chiqarish

-guilloche naqshlari

-iris nashri

-UV ko'rinadigan bo'yoqlar

Bo'rttirma (shtamplash) - bo'rttirma zonalarida joylashtirilgan ma'lumotlar vizual o'qish va optik aniqlash, shuningdek, soxtalashtirishdan himoya qilish usuli sifatida kontaktli nusxa ko'chirish (ya'ni, bosma nashrlardan foydalanish) orqali nashrlarni olish uchun mo'ljallangan;

-golografik laminatsiya

-egasining asl imzosi - plastik kartaning orqa tomonida joylashgan imzo tasmasi qalbakilashtirishdan qo'shimcha himoya vazifasini o'taydi.

kartaning murakkab nostandart shakli - bu juda kam uchraydigan hodisa, zımbalama kalıplarının yuqori narxi tufayli u ko'pincha nostandart plastik mahsulotlarni, masalan, plastik kalit halqalarni ishlab chiqarish bilan shug'ullanadigan tashkilotlarda qo'llaniladi.

-nostandart sirt dizayni (himoya elementlarining mikrogravyurasi bilan laminatsiya oynalaridan foydalanish, maxsus plastmassa turlariga, masalan, lentikulyarlarga bosish), teksturali laminatsiya plyonkalaridan foydalanish

Plastik kartadagi pullarni firibgarlardan qanday himoyalash mumkin?

IIV ma’lumotiga ko’ra, plastik kartalardan pul o‘g‘irlash va firibgarlik holatlari hozirgi vaqtda eng ko‘p sodir etiladigan jinoyatlar qatoriga kiradi. 2021-yilda 2700 dan ortiq o‘zbekistonlik internet firibgarlari qurboni bo‘lgan.

Odamlarni aldash va ularning bank kartalaridan pul o'g'irlashning turli usullari mavjud: bankomat orqali operatsiyalarni amalga oshirish paytida kodni ko’rib olish va kartani o'g'irlashdan tortib, dasturiy ta'minotga xakerlik hujumlarini uyushtirishgacha. Jinoyatchilar pul o'g'irlashning eski usullari ish bermay qo’yganda yangi usullarini o’ylab topishadi. Shunung uchun firibgarlar qo’llaydigan asosiy usullardan xabardor bo'lish va xavfsizlik qoidalariga rioya qilish juda muhimdir.

Bank kartalari hayotimizga mustahkam kirib kelganligi sababli, xavfsizlik bo'yicha mutaxassislar barcha karta egalariga o'zlarining bank kartalari va uning ma'lumotlarini hamyondagi naqd puldan ham qat'iyroq himoya qilishni maslahat berishadi.

Biroq bankning axborot xavfsizligi tizimlariga qaramasdan, firibgarlik operatsiyalari natijasida kartadagi pul mablag'larini o'g'irlash ehtimoli mavjud. Bunga yo'l qo'ymaslik uchun mablag'laringiz bilan noqonuniy operatsiyalar amalga oshirilishidan himoyalaydigan qoidalarga amal qiling:

1-qoida. Parol va kodlaringizni hech kimga aytmang.

Kartadagi PIN-kod hech kimga oshkor etilmaydigan sirdir. Uni telefonda saqlash yoki kartaga yozib qo’yish mumkin emas. Bankomat yoki do'konda PIN-kodni kiritishda klaviaturani qo'l bilan yopish kerak.

Shuningdek, VISA kabi xalqaro kartalarning orqa tomonida CVC / CVV kodi - uchta maxfiy raqam mavjud. Ular onlayn xaridlar amalga oshirishda ishlatiladi. Firibgarlar sizning kartangizdan pul o’g’irlashini oldini olish uchun CVC / CVV kodini hech kimga ko'rsatmang va aytmang.

Bank xodimlari hech qachon kartadagi kodni, PIN-kodni, shuningdek, bank tomonidan yuborilgan SMS- kodlarni so'ramaydi. Faqat firibgarlar maxfiy kodlar bilan qiziqadi. Firibgarlar o‘zlarini go‘yoki sizning kartangizga pul o‘tkazmoqchi bo‘lgan tanishlaringiz deb ko‘rsatishi ham mumkin. Lekin pul o'tkazish uchun ular karta raqami, uning amal qilish muddati yoki CVC/CVV kodini so’rashadi. Bu ham firibgarlik. Pul o'tkazish uchun karta raqamini o’zi kifoya. Boshqa ma'lumotlar - amal qilish muddati, egasining ismi yoki kodi - talab qilinmaydi.

2-qoida. Karta bo’yicha SMS ogohlantirish xizmatini ulang.

Bu xizmat kartadagi barcha harakatlar haqida bankdan SMS-xabarni darhol olish uchun kerak. Masalan, karta orqali to'lanadigan barcha xaridlar haqida ma’lumot olish

uchun. Ushbu xabarlar juda diqqat bilan o'qilishi kerak. Agar siz amalga oshirmagan xarid haqida xabar olgan bo'lsangiz, ehtimol firibgar kartadan foydalangan.

Siz darhol bankka qo'ng'iroq qilishingiz, shubhali SMS haqida xabar berishingiz va kartani blokirovka qilishni so'rashingiz kerak. Bankning ishonch telefoni raqami kartaning orqa tomonida yoziladi. Ushbu raqamni telefoningizdagi kontaktlar ro'yxatiga kiritib qo’ying va karta bilan bog'liq muammolar bo'lsa, shu raqamga qo'ng'iroq qiling.

3-qoida. Xavfsiz saytlarni tanlang.

Firibgarlar mashhur onlayn resurslarning dublikat saytlarini yaratadilar. Masalan, ular bank veb-sayti yoki mobil ilovasining nusxasini yaratishlari mumkin. Agar siz u erda parollar, kodlar, karta ma'lumotlarini kiritsangiz, ular firibgarlarning qo'liga tushadi.

Saytni qanday tekshirish mumkin?

Odatda firibgarlar tomonidan yaratilgan saytlar nomi ba'zi bir taniqli sayt nomi bilan deyarli bir xil bo'ladi, faqat bir nechta harfda farq qilishi mumkin. Shuning uchun siz har doim brauzeringizning manzil satrini diqqat bilan tekshirishingiz kerak.

Resurs manziliga e'tibor bering. Xavfsiz sayt https:// bilan boshlanadi. Xavfsiz saytning manzil satrining oxirida yopiq qulf belgisi mavjud. Agar sayt xavfsiz bo'lmasa, unda shaxsiy ma'lumotlar va karta ma'lumotlarini kiritish mumkin emas.

Har qanday saytga karta yoki pasport ma'lumotlarini kiritishdan oldin uni diqqat bilan o'rganish, internetdagi sharhlarni maqsadga muvofiq bo’ladi.

4-qoida. SMS orqali kelgan shubhali havolalarni bosmang.

Hech qachon notanishlardan kelgan elektron pochta va SMSlardagi havolalarni bosmang. Ko'pincha, bunday havolalar qandaydir pul yutuqlari, yutuqli tanlov

o'tkazilishi yoki mukofot to'lash haqida xabar bilan yuboriladi. Bilingki, agar bunday hollarda sizning kartangiz ma'lumotlari talab qilinsa, bular, albatta, firibgarlardir.

5-qoida. Ma'lumotlarni qayta-qayta tekshiring.

Firibgarlar haqiqatan ham ularga darhol ishonishingizga umid qilishadi. Ma'lumotni ikki marta tekshirishga vaqt bermaslik uchun ular sizni ataylab shoshtirishadi. Ammo pul masalasida shoshilmaslik kerak.

Firibgarlar quyidagi sxemalardan ham foydalanadilar:

Notanish odam qo'ng'iroq qiladi va sizning biror qarindoshingiz yoki do'stingiz muammoga duch kelganini aytadi. Firibgar ularga yordam berish uchun sizdan zudlik bilan pul o'tkazishingizni so'raydi. U sizni qo'rqib, aldanib qolishingizga umid qiladi. Pul o'tkazishga shoshilmang: avval qarindoshlaringizga yoki do'stlaringizga qo'ng'iroq qilib xabar oling.

Sizga pul o'tkazilganligi haqida SMS keladi. Xabar bankdan kelgan xabarga o'xshaydi. Shu zahoti notanish odam sizga qo'ng'iroq qilib, pulni noto'g'ri o'tkazganini aytadi va ularni qaytarishni so'raydi. Ehtimol, bu firibgar, sizga hech qanday pul kelmagan va "bankdan" kelgan SMS esa soxta. Bankka qo'ng'iroq qiling va hisobingizga pul tushganligi haqida so'rang.

Shuni unutmangki, firibgarlar doimiy ravishda aldashning yangi sxemalarini ixtiro qilishadi. Hech qanday holatda kartadagi maxfiy ma'lumotlarni hech kimga - hatto o'zini bank xodimi sifatida tanishtirgan kishiga ham bermang. Vaziyatni tushunmaguningizcha hech qachon pul o'tkazmang. Bankning rasmiy ishonch telefoni raqamiga o'zingiz qo'ng'iroq qiling va sizni qiziqtirgan ma'lumotlarni aniqlang. Asosiysi - shoshilmang.

Xulosa

Plastik kartangiz xavfsizligi uchun ba'zi ehtiyot choralarini ko'rishingiz mumkin:

1. Kartangizning PIN (shaxsiy identifikatsiya raqami) kodini hech kimga bermang va uni xavfsiz joyda saqlamang.
2. Agar siz kartangizni yo'qotib qo'ysangiz yoki u o'g'irlansa, darhol bankingizga xabar bering va kartangizni blokirovka qiling.
3. Onlayn xarid qilish uchun xavfsiz saytlarni tanlang va kartangiz ma'lumotlarini baham ko'rishda ehtiyot bo'ling.
4. Bankomatlardan foydalanayotganda, agar atrofda shubhali vaziyatlar bo‘lsa, ehtiyot bo‘ling va bankomatlardagi kartani o‘qish moslamalari kartangiz nusxalanishiga ishonchli ekanligiga ishonch hosil qiling.
5. Ruxsatsiz tranzaksiyalarni payqash uchun kredit kartangizdan ko‘chirmalarni muntazam tekshirib turing va ularni darhol bankingizga xabar qiling.

Ushbu chora-tadbirlar plastik kartangiz xavfsizligini oshirishga yordam beradi.

Adabiyotlar ro‘yxati:

1. https://uz.wikipedia.org/wiki/Plastik_kartochkalar,
2.https://arxiv.uz/uz/documents/slaydlar/iqtisodiyot/plastik-kartochkalar-haqida-umumiy-ma-lumot