TBC Bank

Firibgarlardan himoyalanish uchun maslahat va tavsiyalar

(Bank kartalaridan foydalanishda xavfsizlik bo‘yicha qo‘llanma)

Texnologik taraqqiyot va raqamlashtirish davrida firibgarlar tobora ko‘proq aldov va yolg‘on yo‘li bilan foyda ko‘rishga urinmoqda. “TBC Bank” ATB (keyingi o‘rinlarda – “Bank”) har bir mijozga quyidagi maslahatlarga amal qilishni tavsiya qiladi:

Ikkita asosiy qoida:

Agar siz qo‘ng‘iroq kutmayotgan va hech qanday amaliyot bajarmagan bo‘lsangiz, ozgina shubha tug‘ilishi bilan go‘shakni qo‘ying va bankingiz rasmiy saytida yoki bank kartasida ko‘rsatilgan raqamga qaytadan qo‘ng‘iroq qiling.

Agar sizdan shoshilinch yordam so‘rashsa, so‘rov yuborgan kishining o‘zi bilan shaxsan bog‘laning (qo‘ng‘iroq qiling, xabar yozing, yuzma-yuz ko‘rishing) va yaqin insoningiz haqiqatan ham yordamga muhtojligi, nima bo‘lganini aniqlashtiring.

1. Xavfsizlikning asosiy qoidalari

- SMS kodlarni hech qachon hech kimga aytmang. Bank xodimlari sizdan aslo bunday ma’lumotlarni so‘ramaydi.
- Siz bajarmagan karta amaliyotlarini hech qachon tasdiqlamang.
- Notanish raqamlar qo‘ng‘iroqlariga javob bermang va suhbatdosh o‘zini Bank xodimi deb tanishtirsa ham, telefon orqali ma’lumotlaringizni bermang. Bankdan doim sizga +998 78 777 27 27 raqami orqali telefon qiladi.
- Soxta tanlov va yutuqli o‘yinlardan ehtiyot bo‘ling. Bank aksiyalari faqat Bankning rasmiy kanallari yoki ilovasida o‘tkaziladi.
- Notanish yoki tekshirilmagan to‘lov xizmatlari orqali xarid qilmang. Begona saytlarda bank kartasi ma’lumotlari (karta raqami, amal qilish muddati, CVV kod) so‘ralgan anketalarni to‘ldirmang.

2. Firibgarning uchta asosiy belgisi

1) Sizga noma’lum yoki yashirin raqamdan qo‘ng‘iroq qiladi;
2) Kartangizni buzib kirishga urinishayotgani haqida noma’lum raqamdan SMS yuboradi;
3) Karta raqami, uning amal qilish muddati, CVV (kartaning orqa tomonidagi uchta raqam) yoki SMS kodlarni aytishingizni so‘raydi.
Agar sizga shunday SMS kelsa yoki qo‘ng‘iroq bo‘lsa — bu firibgar.

Firibgarlikning asosiy belgilari:

- Shoshilinch va vaqt bosimi bo‘ladi (“tezda harakat qilish kerak”, “sizda 5 daqiqa vaqt qoldi”).
- Tez va oson daromad, lotereyada yutuq yoki noodatiy foydali shartlarni va’da qilishadi.
- Oqibatlar bilan qo‘rqitishadi (“hisobraqamingiz bloklanadi”, “nomingizga kredit olingan”, “jinoiy ish ochilgan”).

3. Onlayn savdo platformalaridagi firibgarlik

- Firibgarlar savdo platformalaridagi sotuvchilarga qo‘ng‘iroq qilib, karta raqami, uning amal qilish muddati va SMS kodni so‘rashadi. Kodni aytsangiz — pulingizdan ayrilasiz.
- Kartangiz rasmini hech kimga yubormang. Karta ma’lumotlari (karta raqami — 16 ta raqam, amal qilish muddati va CVV kod) firibgarlik uchun ishlatilishi mumkin.

4. Ijtimoiy tarmoqlar va ilovada himoyalanish

- Bankning barcha xizmatlaridan faqat TBC UZ mobil ilovasi yoki Bankning www.tbcbank.uz rasmiy veb-sayti orqali foydalanish mumkin. Boshqa ijtimoiy tarmoqlar, messenjerlar yoki o‘zga norasmiy kanallar orqali keladigan takliflarga ishonmang. Shuningdek, shubhali havolalarga kirmang va shaxsiy ma’lumotlaringizni uchinchi shaxslarga bermang.
- Uchinchi shaxslar ta’sirida kredit olmang — nomingizga olingan hamma kreditlar uchun mas’uliyat sizning zimmangizda bo‘ladi.
- Firibgarlikni sezganda, darhol TBC UZ mobil ilovasida bank kartasini bloklang va Bankka quyidagi raqam orqali qo‘ng‘iroq qiling: +998 78 777 27 27.
- Ijtimoiy tarmoqlarda shaxsiy ma’lumotlarni (tug‘ilgan sana, manzil, yaqinlaringiz ismlari, hujjatlar suratlari) joylamang. Firibgarlar bu ma’lumotlardan ijtimoiy muhandislik, parollarni topish va ishonchli aldov ssenariylarini yaratish uchun foydalanadi.

5. Bankomatlardan foydalanishda xavfsizlik choralari

- Faqat bank filiallari, davlat tashkilotlari, savdo markazlari va videokuzatuv tizimi bo‘lgan joylarda bankomatlardan foydalaning.
- Bankomatning klaviaturasi va kartani qabul qilish joyida begona qurilmalar (ustki nakladka), ya’ni skimming belgilari yo‘qligini tekshiring.
- PIN kodni kiritganda klaviaturani qo‘lingiz bilan to‘sing. PIN kodni kartaning o‘zi yoki uning yoniga yozib qo‘ymang.
- Bankomat kartani qaytarmasa, uning yonidan ketmang va darhol Bankka quyidagi raqam orqali qo‘ng‘iroq qiling: +998 78 777 27 27.

6. Raqamli xavfsizlik va qurilmalarni himoyalash

- TBC UZ mobil ilovasini faqat rasmiy manbalardan (App Store / Google Play) o‘rnating. Ilovalarni SMS yoki messenjerlardagi havolalar orqali yuklab olmang.
- Operatsion tizim va ilovalarni muntazam yangilab turing. Ilovaga kirish uchun qiyin parol yoki biometrik ma’lumotlardan (barmoq izi, Face ID) foydalaning.
- Bank ilovasi va boshqa xizmatlar uchun bir xil parollarni ishlatmang.
- Ommaviy Wi-Fi tarmoqlaridan (kafe, aeroport va boshqa jamoat joylari) foydalanib bank amaliyotlarini bajarmang. Xavfsizlik darajasini oshirish uchun mobil internetdan foydalaning.
- Smartfoningiz yo‘qolsa yoki o‘g‘irlansa, darhol Bankka xabar berib, mobil ilovaga kirishni bloklang.
- Smartfon va kompyuteringizga antivirus o‘rnating.

7. Ijtimoiy muhandislikdan himoyalanish

- Firibgarlar o‘zlarini bank, militsiya, soliq yoki boshqa tashkilotlarning xodimi sifatida tanishtiradi. Haqiqiy xodimlar hech qachon PIN kod, CVV yoki SMS kodlarni so‘ramaydi.
- “Hisobraqamingiz bloklandi”, “shubhali operatsiya” kabi bosimlarga ishonmang. Suhbatni yakunlab, Bankka rasmiy aloqa kanallari orqali qo‘ng‘iroq qiling yoki yozing.
- Shubhali SMS yoki e-mailda kelgan havolalarga (fishing) kirmang. Telegram va WhatsApp’dagi shubhali “foydali” takliflardan ehtiyot bo‘ling.

8. Onlayn to‘lovlar xavfsizligi

- Faqat tekshirilgan saytlardan (qulf belgisi, https://) xarid qiling. Karta ma’lumotlarini brauzerlarda saqlamang.
- Onlayn xaridlar uchun asosiy karta o‘rniga cheklangan limitli virtual kartadan foydalaning.
- Barcha operatsiyalar bo‘yicha SMS xabarni yoqib qo‘ying. Tasdiqlash kodini olganda operatsiya summasi va qabul qiluvchini tekshiring.
- Jamoat joylaridagi (restoranlar, avtoturargohlar, bekatlar) QR kodlardan ehtiyot bo‘ling. Firibgarlar asl QR kodlarni to‘lov sahifalariga o‘xshash fishing saytlariga olib boradigan stikerlar bilan almashtirib qo‘yishadi. QR kod orqali to‘lov qilishdan oldin, havola to‘lov xizmatining rasmiy domeniga olib borishini tekshiring.

9. Kreditlarning firibgarlik yo‘li bilan olinishidan himoyalanish

- Pasport, JSHSHIR yoki hujjatlaringiz nusxalarini notanish shaxslarga bermang. Kredit tarixingizni doim tekshirib turing.
- Agar sizga olingan kredit haqida xabar kelsa, tezda bank va huquqni muhofaza qilish organlariga murojaat qiling.

Firibgarlik holatiga duch kelsangiz, nima qilish kerak?

1. Kartani darhol TBC UZ mobil ilovasi orqali yoki +998 78 777 27 27 raqamiga qo‘ng‘iroq qilib bloklang.
2. Huquqni muhofaza qilish organlariga ariza bilan murojaat qiling.
3. Bankka ruxsatsiz bajarilgan operatsiyalar haqida ariza yozing.
4. Dalillarni saqlab qo‘ying: skrinshotlar, yozib olingan qo‘ng‘iroq, SMS xabar.
5. incident_compliance@tbcbank.uz elektron pochta manziliga yoki +998 78 777 27 27 raqamiga qo‘ng‘iroq qilib holat haqida xabar bering.

TBC Bank

Советы и рекомендации для защиты от мошенников

(Руководство по безопасности при использовании банковских карт)

В эру технологического развития и цифровизации всё больше мошенников пытаются найти способы выгоды за счёт обмана и махинаций. АКБ «TBC Bank» (далее – «Банк») призывает каждого клиента соблюдать следующие рекомендации:

Два главных правила:

Если вы не ожидали звонка и не совершали никаких операций, то при малейшем сомнении положите трубку и перезвоните по номеру вашего банка, указанному на официальном сайте или на банковской карте.

Если вас просят о срочной помощи, обязательно свяжитесь с инициатором запроса лично (звонок, сообщение, личный контакт) и уточните, действительно ли вашему близкому нужна помощь и что именно произошло.

1. Основные правила безопасности

- Никогда и никому не сообщайте коды из СМС. Сотрудники Банка никогда не запрашивают такие данные.
- Никогда не подтверждайте транзакции по карте, которые вы не совершали.
- Не отвечайте на звонки с незнакомых номеров и не делитесь данными по телефону, даже если собеседник представляется сотрудником Банка. Все звонки от Банка осуществляются по номеру +998 78 777 27 27.
- Остерегайтесь фальшивых конкурсов и розыгрышей. Акции Банка проводятся только в официальных каналах Банка или приложении.
- Не совершайте покупки через неизвестные или непроверенные платёжные сервисы. Не заполняйте формы на сторонних сайтах, где просят данные банковской карты (номер карты, срок действия, CVV-код).

2. Три главных признака мошенника

1) Вам звонят с неизвестного либо скрытого номера;
2) Отправляют СМС с неизвестного номера о том, что вашу карту пытаются взломать;
3) Просят сообщить номер карты, срок действия, CVV (три цифры на обратной стороне карты) или коды из СМС.

Если вы получили такое СМС или звонок — вы имеете дело с мошенником.

Характерные признаки мошенничества:

- Создают ощущение срочности и давления по времени («нужно действовать немедленно», «у вас осталось 5 минут»).
- Обещают быстрый и лёгкий заработок, выигрыш в лотерее или необычно выгодные условия.
- Запугивают последствиями («ваш счёт будет заблокирован», «на вас оформлен кредит», «возбуждено уголовное дело»).

3. Мошенничество на онлайн-торговых площадках

- Мошенники звонят продавцам на торговых площадках, просят номер карты, срок действия карты, а затем код из СМС. Сообщив код — вы теряете деньги.
- Не делитесь фотографией карты. Данные карты (номер карты — 16 цифр, срок действия и CVV-код) могут быть использованы для совершения мошеннических операций.

4. Защита в социальных сетях и приложении

- Все банковские услуги Банка предоставляются только через мобильное приложение TBC UZ или официальный веб-сайт Банка www.tbcbank.uz. Не доверяйте предложениям, поступающим через сторонние социальные сети, мессенджеры или иные неофициальные каналы. А также не переходите по подозрительным ссылкам и не передавайте свои персональные данные третьим лицам.
- Не оформляйте кредит под влиянием третьих лиц — все кредиты на ваше имя, являются вашей ответственностью.
- При подозрении на мошенничество рекомендуется немедленно заблокировать банковскую карту в мобильном приложении TBC UZ и позвонить в Банк: +998 78 777 27 27.
- Ограничьте публикацию личной информации в социальных сетях (дата рождения, адрес, имена близких, фотографии документов). Мошенники используют эти данные для социальной инженерии, подбора паролей и создания убедительных сценариев обмана.

5. Безопасность при использовании банкоматов

- Пользуйтесь банкоматами в отделениях банков, государственных учреждениях, торговых центрах и местах с системой видеонаблюдения.
- Проверяйте банкомат на отсутствие посторонних устройств (накладок) на клавиатуре и картоприёмнике (признаки скимминга).
- Прикрывайте клавиатуру рукой при вводе пин-кода. Не записывайте пин-код на карте или рядом с ней.
- Если банкомат не вернул карту — не отходите от банкомата и сразу звоните в Банк по номеру: +998 78 777 27 27.

6. Цифровая безопасность и защита устройств

- Устанавливайте мобильное приложение TBC UZ только из официальных источников (App Store / Google Play). Не скачивайте приложения по ссылкам из СМС или мессенджеров.
- Регулярно обновляйте операционную систему и приложения. Используйте сложный пароль или биометрию (отпечаток пальца, Face ID) для входа.
- Не используйте одинаковые пароли для банковского приложения и других сервисов.
- Не проводите банковские операции с использованием публичных Wi-Fi сетей (кафе, аэропорты и иные общественные места). Используйте мобильный интернет для повышения уровня безопасности.
- При утере или краже смартфона рекомендуется немедленно уведомить Банк и заблокировать доступ к мобильному приложению.
- Установите антивирусное приложение на смартфон и компьютер.

7. Защита от социальной инженерии

- Мошенники представляются сотрудниками банка, полиции, налоговой и иных организаций. Настоящие сотрудники никогда не запрашивают пин-коды, CVV или коды из СМС.
- Не поддавайтесь давлению («счёт заблокирован», «подозрительная операция»). Завершите разговор по телефону, позвоните или напишите в Банк по официальным каналам связи.
- Не переходите по ссылкам из подозрительных СМС-уведомлений/email (фишинг). Будьте осторожны с подозрительно «выгодными» предложениями в телеграме и WhatsApp.

8. Безопасность онлайн-платежей

- Покупайте только на проверенных сайтах (символ замка, https://). Не сохраняйте данные карты в браузерах.
- Для онлайн-покупок используйте виртуальную карту с ограниченным лимитом вместо основной карты.
- Подключите СМС-уведомления по всем операциям. При получении кода подтверждения рекомендуется проверять сумму операции и получателя.
- Будьте осторожны с QR-кодами в общественных местах (рестораны, парковки, остановки). Мошенники подменяют оригинальные QR-коды наклейками, ведущими на фишинговые сайты, которые имитируют платёжные страницы. Перед оплатой через QR-код убедитесь, что ссылка ведёт на официальный домен платёжного сервиса.

9. Защита от мошеннического оформления кредитов

- Не передавайте паспорт, ПИНФЛ или копии документов незнакомым лицам. Регулярно проверяйте кредитную историю.
- В случае получения уведомления о кредите, который вы не оформляли, рекомендуется немедленно обратиться в банк и правоохранительные органы.

Что делать, если вы стали жертвой мошенников

1. Немедленно заблокируйте карту через мобильное приложение TBC UZ или по номеру +998 78 777 27 27.
2. Подайте заявление в правоохранительные органы.
3. Обратитесь в Банк с заявлением о несанкционированных операциях.
4. Сохраните доказательства: скриншоты, записи звонков, СМС-уведомления.
5. Сообщите о случившемся по адресу электронной почты: incident_compliance@tbcbank.uz или по номеру +998 78 777 27 27.