Шановний клієнте, ми розробили для вас невелику нотатку щодо безпеки користування карткою та мобільним додатком.

Тут не буде нудних формальних правил з розряду "зберігайте гроші під подушкою" або "нікому не передавайте свою картку".
Ми дамо реальні поради, які працюють.

Поїхали!

Безпека мобільного додатка:

1. Перша лінія вашої оборони при втраті або крадіжки смартфону, це встановлене блокування смартфону. Це може бути PIN код, графічний ключ або біометрична ідентифікація. Це ускладнить (так-так, не зупинить) доступ до ваших даних у смартфоні, що дасть вам час для блокування картки.

2. Друге основне правило - не зберігайте PIN код для входу в додаток monobank на вашому телефоні, наприклад в нотатках. Ви посміхнулися? Банальна порада. Однак, багато хто саме так і робить. Порада саме для тих, хто зараз не посміхався;)

3. У разі зміни смартфону, ми відправляємо вам на емейл лист для підтвердження "володіння довіреним пристроєм" (за цією фразою ховається саме ваш смартфон). Пристрій стає довіреним, якщо через отриманий лист підтвердити, що це ваш пристрій або почекати добу. Поки пристрій не стане довіреним, діють ліміти на витрати (для фізичної карти ліміти не встановлюються).
Схема абсолютно стійка до перевипуску SIM карти, тому що зловмисник не знає PIN і серійного номеру пристрою клієнта. Навіть не переймайтеся тим, що хтось може заволодіти вашою сімкою, у нас за весь час не було інцидентів з втратою грошових коштів від перевипуску сім карти.

4. Ми розробили Центр Безпеки, щоб ви могли самостійно управляти рівнем безпеки вашої картки та додатку mono. Дуже радимо ознайомиться з цим у меню в Мобільному додатку. Нижче наведемо декілька порад та прикладів, як ці налаштування можуть вам допомогти:

Порада №1. Якщо ви хвилюєтесь, що картка могла бути скомпрометована, тобто є ризик, що чутливі дані з картки були зчитані, при поїздці за кордон, можна активувати відповідні налаштування і відхиляти платежі, де країна здійснення платежу не збігається з країною розташування смартфону клієнта.

Порада №2. Якщо ви робите багато покупок в Інтернеті і хвилюєтесь, що картка може бути скомпрометована - маєте можливість використати динамічний cvv код, який буде змінюватися кожні 60 хвилин.

Порада №3. Ви можете відключити оплату магнітною смугою, безконтактну оплату або зняття грошей в банкоматі - відключаючи нетипові для себе сценарії використання карти, ви закриваєте потенційні лазівки і для шахраїв.

Якщо ми бачимо платіж, який повинен бути відхилений згідно налаштувань безпеки, ми відхиляємо його і сповіщаємо вас про це. Також, пропонуємо вам пропустити наступний такий платіж або відключити таке правило.

Безпека картки

5. ~~Не передавайте картку в користування 3м особам.~~ Ми обіцяли про це не писати, тому не пишемо.

6. Втратили / вкрали карту - негайно зверніться в банк для її блокування.

Безпека даних картки

7. Дані карти: CVV код, термін дії, PIN код - потрібні тільки вам для здійснення оплати в Інтернеті. Ніколи (!!!) не передавайте ці дані 3м особам. Навіть якщо вони представилися співробітниками банку, міністром МВС або Президентом США.

8. Якщо ви купуєте в Інтернеті, то ви повинні довіряти тому сайту, на якому вводите дані карти. Наприклад, сайт www.polychite1milliondollarov.com явно фішинговий/шахрайський і його мета зібрати з вас дані карти, щоб потім списати з неї гроші.

Соціальна інженерія

Це найважливіший і одночасно складний блок, тому що саме він є основним каналом у шахраїв до вашої картки.

9. Якщо вам надходить вхідний дзвінок / повідомлення з банку, а не ви самостійно набрали банк або написали банку в звичний месенджер - ніколи нічого не повідомляйте, окрім не шкідливої інформації. Наприклад, питання цікавить вас якась послуга чи ні. Ніяких кодів, ПІН-кодів, паролів, надісланих в SMS. НІЧОГО! Навіть якщо той, хто телефонує представляється службою безпеки і т.д.

10. Якщо вам дзвонять і повідомляють, що з вашої картки списали / списуються гроші і просять назвати дані карти / натиснути кнопку підтвердити в додатку / зробити переказ грошей з вашої картки на "захищену карту" / поповнити Ваш номер телефону - ЦЕ ДЗВОНЯТЬ ШАХРАЇ (!).
Давайте повторимо ще раз - НЕ передавайте дані картки третім особам. Відразу припиняйте з ними телефонний діалог і телефонуйте в банк.

11. Вас будуть квапити передати дані картки, перевести гроші і ще мільйон різних варіантів отримати доступ до ваших грошей. Головне правило - зупиніться, подумайте, самі зв'яжіться з банком і проконсультуйтеся.

12. Родичі в біді. Якщо вам в соціальних мережах пишуть друзі / родичі / знайомі з проханням допомогти грошима - не поспішайте переводити гроші.
Спробуйте перевірити хто саме вам пише. Шахраї можуть зламати акаунт вашого знайомого і намагатися виманити у вас гроші.

Задайте 1-2 запитання, відповіді на які може знати тільки ця людина або наберіть його по телефону, щоб переконатися, що вам пишуть не шахраї.

13. Не вірте пропозиції отримати нічим необґрунтовану вигоду (оплата за участь в опитуваннях, виплати від урядів різних країн, виграш автомобіля і т.д.).
Як відомо "безкоштовний сир тільки в мишоловці". Читаючи або дивлячись відео про "акції / схемою" "мега / 100% го заробітку" - будьте впевнені, що в підсумку вас попросять оплатити "невелику" (або більшу) комісію ввівши дані карти і підтвердивши платіж. І будуть просити до тих пір, поки Ви або не схаменетесь, або у вас не закінчаться гроші на картці.

14. Не вірте пропозиції про продаж товару за заниженою ціною.
Кожен товар має свою ціну і, наприклад, смартфон ціною 15 000 грн, не може продаватися за 7 000 грн. Звичайно, вам може і пощастить і це буде реальна угода, але статистика поки не на користь цього твердження;)
В даному випадку шахраї можуть зажадати від Вас повну передоплату і не вислати товар.
Або відправити вам фейкове посилання на відомий ресурс для оплати (зробити підроблений сайт відомої організації). Після оплати на такому підробленому ресурсі Ви втратите гроші і не отримаєте товар.

15.Укладаючи Договір Сторони зобов'язані виконувати та дотримуватися Політики інформаційної безпеки/кібербезпеки АТ «УНІВЕРСАЛ БАНК», що розміщена на офіційному сайті Банку за посиланням https://www.universalbank.com.ua/our-bank

Якщо ви дочитали до цього абзацу, ви наш герой, а юристи і безпека банку моляться на вас ;)