ПУТІВНИК
У СВІТ ПЛАТІЖНИХ КАРТ

№1

БЕЗПЕКА

КАРТИ, ГРОШІ, ТЕЛЕФОН: БЕЗПЕЧНІ ІНТЕРНЕТ-ПОКУПКИ

Сплата товарів та послуг онлайн вже давно стало нормою повсякденного життя. Швидко, зручно, безпечно, якщо дотримуватися простих правил. Щонайменше не передавати третім особам дані, які може знати тільки власник картки. Інакше це як передати гаманець сторонній людині.

Найчастіше користувачі банківських карт стикаються з шахрайством через розголошення власних конфіденційних даних. Свої паролі та коди вони передають самі, так званим «співробітникам» банку, НБУ, МВС та іншим офіційним організаціям, забуваючи, що ніхто, навіть співробітник банку, не має права запитувати у клієнта банку термін дії його пластикової карти, PIN-код, слово-пароль, cvv2 / cvc2 коди. Ця інформація є конфіденційною, а значить, не підлягає розголошенню.

UKRSIBBANK BNP Paribas Group прагне зробити фінансове життя клієнтів успішним, безпечним і простим.

Тому звертає увагу клієнтів на правила роботи з банківською картою при покупках в інтернеті, а також тактику спілкування з потенційними шахраями.

При здійсненні продажу через інтернет покупцеві, який буде переводити гроші на карту, досить знати тільки номер картки (16 цифр), а також прізвище, ім'я, по батькові власника картки. Термін дії карти, cvv2 / cvc2 коди (цифри на зворотному боці картки) і одноразові коди з SMS покупцю не потрібні в жодному разі. Якщо ви розмістили на дошці оголошення на OLX або іншому майданчику для покупок-продажів номер вашої карт (16 цифр) і потенційний покупець просить у вас три цифри на зворотному боці картки cvv2 / cvc2 і термін дії карти це шахрай. Отримавши ці дані, шахраї можуть скористатися ними для здійснення грошових переказів з вашої картки або власних покупок в Інтернет.

Можливий такий сценарій, Вам зателефонували з так званої служби безпеки банку, сказали, що шахраї намагалися списати гроші, але банку операція здалася підозрілою і потрібно звірити дані Вашої картки — це також шахраї.

Співробітники банку ніколи не запитують номер платіжної картки, її терміни і cvv2 / cvc2.

Такий вид шахрайства називається вішинг — коли зловмисники, представляючись покупцями, співробітниками банку, Пенсійного фонду, НБУ, СБУ, і навіть поліцією виманюють у власника платіжної картки конфіденційну інформацію під приводом звірки даних. За даними експертів, одна така телефонна розмова «коштує» у середньому 5000 гривень.

Щоб не стати жертвою злочинців дотримуйтесь простих правил — в жодному разі нікому не повідомляйте разом з номером своєї карти її секретні реквізити:

1) Термін дії карти;

2) Тризначний код безпеки на зворотній стороні картки (код CVV2 / CVC2), який потрібен для здійснення операцій з платіжною карткою в Інтернет;

3) Паролі з смс-повідомлень від банку, які потрібні для підтвердження операцій з карткою (якщо карта захищена по системі 3D Secure).

Номер своєї банківської картки ви можете повідомляти, коли, наприклад, продаєте щось, отримуєте грошову винагороду або благодійну допомогу. Але вказати можна тільки номер карти. Інші реквізити для здійснення грошового переказу на вашу карту не потрібні.

Дотримання таких нескладних, але дуже важливих правил, дозволить кожному клієнту банку відчувати себе впевнено і спокійно при роботі з платіжними картами.

БЕЗПЕКА ІНТЕРНЕТ-БАНКІНГУ

З розвитком інформаційних технологій ми все частіше використовуємо інтернет-банкінг для здійснення електронних платежів. Водночас кіберзлочинці почали використовувати нову схему з метою проведення шахрайських операцій по платіжних картках. Шахраї можуть здійснити несанкціонований вхід до інтернет-банкінгу за допомогою сім-картки, до якої підв'язаний інтернет-банкінг її власника. Для цього вони блокують сім-картку, поки її власник з'ясовує, чому сім-картку заблоковано, шахраї телефонують на гарячу лінію оператора мобільного зв'язку, «відновлюють» сім-картку та отримують доступ до всіх повідомлень, які на неї приходять — смс-повідомлень з секретними кодами та паролями від банку, а також до інших даних, прив'язаних до номеру телефону, зокрема, це можуть бути: електронна пошта, соціальні мережі тощо.

Якщо ви помітили, що ваш номер мобільного телефону перестав працювати негайно зверніться:

1) У банк для блокування платіжних карток, які прив'язані до номеру телефону;

2) До мобільного оператора для уточнення подальших дій.

Щоб запобігти крадіжці мобільного номеру у майбутньому, зверніться до мобільного оператора та відключіть можливість віддаленого перевипуску своєї sim-картки.

У такому випадку, навіть якщо кіберзлочинцям вдасться заблокувати Вашу картку, то відновити її можна буде лише за документами, за якими закріплений номер.

ОСНОВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Шановні клієнти, дбайте про конфіденційність ваших даних у соціальних мережах — будьте пильні при додаванні друзів та у персональній переписці.

Нагадуємо, що UKRSIBBANK BNP Paribas Group пише своїм клієнтам виключно з офіційної сторінки. Жодна людина зі своєї особистої сторінки не може звертатися до вас з питаннями і пропозиціями від імені банку.

Якщо вам в Facebook Messenger надходять повідомлення нібито від імені банку з пропозицією отримати кредит на вигідних умовах, пам'ятайте про захист своїх даних. Насправді мета подібних повідомлень одна — отримати конфіденційні дані клієнтів банків та доступ до банківських рахунків, BankID, Google акаунта, пошти, Viber, облікових записів у соцмережах та месенджерах, фото та відео із подальшою крадіжкою коштів, шантажу або іншими злочинними намірами.

В жодному разі не повідомляйте третім особам конфіденційні дані банківських платіжних карт і паролі з SMS-повідомлень. Співробітники UKRSIBBANK ніколи не будуть надавати запит на подібні дані у своїх клієнтів.

УВАГА!

У разі виникнення будь-яких питань, просимо звертатись за детальною консультацією до співробітника UKRSIBBBANK, який знаходиться за адресою: вул Криворожсталі 1, приміщення будівлі Університету АрселорМіттал Кривий Ріг.

Графік роботи:
понеділок з 8.00 до 17.00
четвер з 8.00 до 17.00

Або зателефонуйте до контакт центру UKRSIBBANK BNP Paribas Group:

0 800 505 800 (безкоштовно в межах України);

380 44 590 06 90 (для міжнародних дзвінків).