Альфа дайджест

№13 / лютий 2018

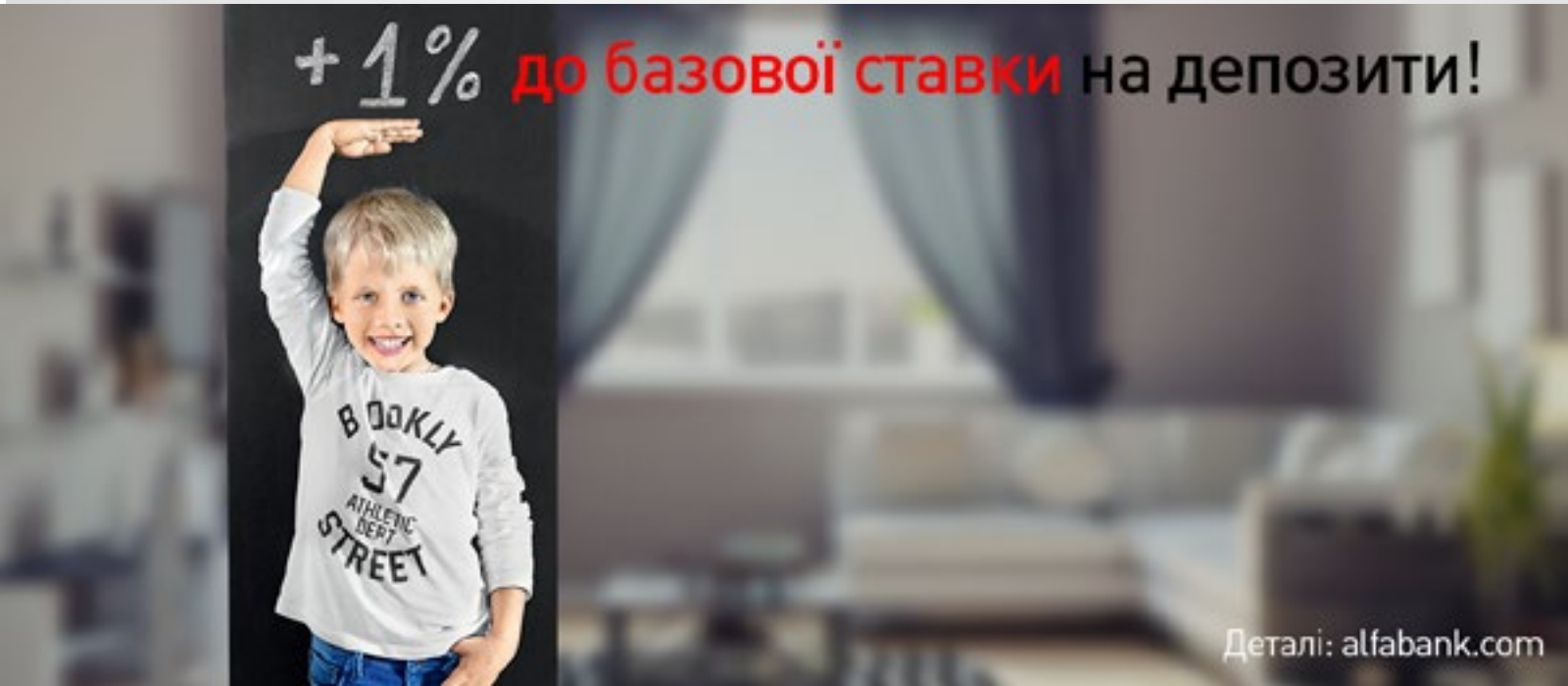
Електронний випуск для власників зарплатих карток

У ЦЬОМУ НОМЕРІ:

ПЕРЕКАЗУЙТЕ КОШТИ ЗА **НОМЕРОМ МОБІЛЬНОГО** АБО **E-MAIL**

Альфа-Банк Україна доповнив сервіс переказів з карти на карту **p2p.alfabank.ua** можливістю миттєво переказувати кошти по Україні, вказавши лише **номер мобільного** або **e-mail отримувача**, без необхідності пам'ятати номер карти отримувача.

При такому переказі отримувачу відправляється відповідне посилання через **SMS** або **e-mail**, переходячи за яким він вказує номер своєї карти, зручної для зарахування коштів. Підтвердження отримання можливе протягом 4-х календарних днів. Після цього кошти автоматично повертаються на карту відправника, у тому числі комісія. Це є однією з ключових переваг цього сервісу, що робить перекази максимально **безпечними як для відправника, так і отримувача.**



Телефонний вішинг. Не дати витягнути секретні дані, або Як вберегтися від зловмисників?

За статистикою, понад 70% власників карток під психологічним тиском шахраїв розголошують конфіденційні дані та стають жертвами обману.

Уявімо ситуацію: до вас підходить незнайомець та просить віддати йому ключі від квартири або машини чи, скажімо, назвати код сигналізації будинку. Ваші дії? Звичайно, ви відмовите та підете геть, покрутивши пальцем біля скроні.

З банківською картою точно так само – якщо незнайомці намагаються дізнатися про секретні дані, ви повинні відмовити, не роздумуючи. Не варто лякатися чи відмовлятися від карти, адже вона дійсно набагато зручніша за гаманець – з її допомогою можна купувати в інтернеті, бронювати номери в готелях, при цьому не носити з собою великі суми готівкою, наражаючи себе цим на значно більшу небезпеку. Просто дотримуйтесь простих правил, які ми розглянемо нижче, і ваша карта буде в безпеці.

Ми зібрали найрозповсюдженіші схеми вішингу у цій статті, щоб ви завжди були готові, якщо на ваш телефон надійдуть сумнівні SMS або дзвінки.

«Продавець – покупець»

Суть схеми базується на взаємовідносинах продавця та покупця товару, оголошення про який розміщується на популярних дошках безкоштовних оголошень в інтернеті.

Живий приклад:

Клієнт опублікував приватне оголошення про продаж товару із зазначенням особистого мобільного номера.

Шахраї під виглядом покупців зв'язуються з клієнтом та виявляють бажання нібито придбати товар і відразу перерахувати за нього передоплату.

За якийсь час шахраї під виглядом співробітників банку зв'язуються з клієнтом та повідомляють, що йому на карту планується до зарахування грошовий переказ, але без спеціального коду підтвердження, який прийде в SMS, він неможливий.

Клієнт повідомив у телефонній розмові цей код, який насправді був кодом підтвердження зміни паролю до облікового запису в системі інтернет-банкінгу...

Шляхом аналогічних маніпуляцій шахраї спонукають клієнта повідомити інші коди підтвердження, що надійшли йому в SMS, які необхідні для здійснення різних операцій через систему інтернет-банкінгу.

У результаті з двох карт клієнта було здійснено перекази на карти іншого банку на сумув межах **65-66 тисяч грн.**

Загалом розмова шахраїв з клієнтом тривала близько 1 години. Клієнт весь цей час знаходився за кермом.

«Служба безпеки»

Ця схема найбільш популярна. Її суть в офіційному характері відносин клієнта та банку.

Живий приклад:

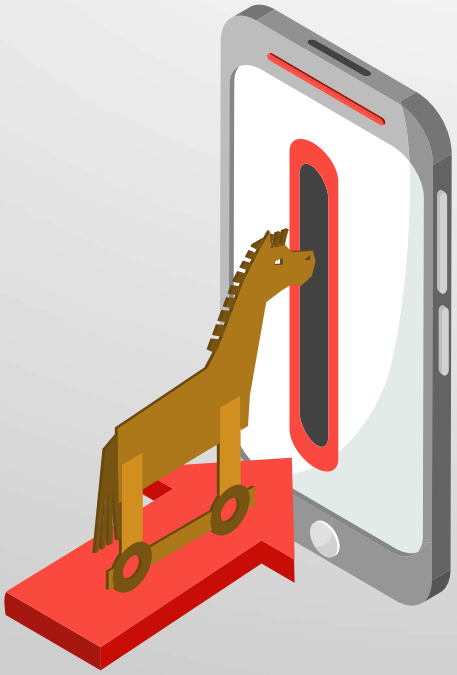
Клієнту на мобільний надійшов дзвінок з невідомого номера. Той, хто дзвонив, представився співробітником служби безпеки банку та повідомив, що карта клієнта заблокована внаслідок спроб шахрайських операцій по карті.

Далі зловмисник запропонував клієнту підключити до функціоналу карти «4-й рівень захисту від несанкціонованих операцій», для чого необхідно повідомити номер карти, строк дії та «номер відділення, у якому було видано карту – його нанесено у вигляді 3-х цифр на зворотному боці карти» (насправді – це CVV-код).

Використовуючи отримані дані, шахраї вивели з карти клієнта кошти на загальну суму в межах **43-44 тисяч грн**.

Шахраїв не обов'язково можуть цікавити реквізити карти, вони також можуть виманювати коди підтвердження з SMS, попередньо відправлених клієнту.

Також не обов'язково шахрай може представлятися співробітником служби безпеки банку – варіанти можуть бути дуже різні: служба підтримки клієнтів, співробітник НБУ, поліції, СБУ, прокуратури, платіжної системи тощо.



Щоб не попастися на хитрощі та ненароком все-таки не видати бажану для шахраїв інформацію, потрібно знати і завжди пам'ятати:

1. Співробітники банку мають доступ до всієї необхідної інформації та **ніколи не запитують реквізити карти через телефон та інтернет**.

2. Перерахування коштів на карту відбувається без будь-якої участі її власника, для цього **необхідний лише номер карти**. Жодних додаткових даних нікуди вводити і нікому повідомляти не треба.

3. Єдині номери телефонів, за якими можна зв'язатися зі співробітниками банку, надруковані **на зворотному боці карти або розміщені на офіційному сайті банку**. Із будь-якими запитаннями потрібно звертатися **тільки за цими номерами**, а не за номерами, надісланими в SMS або отриманими зі сторонніх джерел.

4. Якщо клієнт має кредитну карту банку, то питання про збільшення кредитного ліміту повинно вирішуватися **лише в цьому банку, а не в сторонніх організаціях або за оголошеннями.**

5. Якщо виникли найменші підозри стосовно легітимності дзвінка з банку, то цілком прийнятною і правильною буде така лінія поведінки: скориставшись будь-яким приводом, **припинити розмову та передзвонити в банк за номерами контакт-центру**, щоб уточнити інформацію про цей дзвінок.

Нагадуємо, номер гарячої лінії Альфа-Банку Україна: **0 800 50 20 50** (цілодобово, безкоштовно з мобільних по Україні) і **+38 (0462) 616 111** (для дзвінків з-за кордону).

Будьте пильними!