УКРБУДІНВЕСТБАНК

БЕЗПЕКА ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ КЛІЄНТІВ

БЕЗПЕКА КЛІЄНТІВ – ЦЕ ГОЛОВНЕ ЗАВДАННЯ ДЛЯ НАШОГО БАНКУ

Ми живемо у суспільстві, що щвидко розвивається та без електронних платіжних засобів нажаль не можливо обійтись отже, виникає необхідність у використанні систем дистанційного управління рахунками. Для задоволення таких потреб банки на своїх сайтах розміщують сервіси, що можуть не тільки полегшити виконання повсякденних операцій з рахунками, але і забовольнити потреби найвибагливіших клієнтів.

Нажаль, використання таких сервісів пов'язане з низкою ризиків. Але уникнути негативних наслідків використання Клієнтами банківських систем дистанційного обслуговування можливо завдяки ознайомленню з деякими базовими Правилами інформаційної безпеки.

ПРАВИЛА ТЕЛЕФОННИХ РОЗМОВ

Шахрайські дії найчастіше здійснюються з використанням телефонного дзвінку, для отримання конфіденційної інформації або спроб вплинути на людину.

Особа, яка Вам зателефонувала, може представитись співробітником Банку, представником страхової компанії або службою безпеки Банку. В таких випадках необхідно негайно зателефонувати на номери, вказані на офіційній вебсторінці Банку.

Шахраї під час телефонної розмови:

- запитують login та\або пароль до систем дистанційного обслуговування;

- запитують Ваші персональні та конфіденційні дані;

- пропонують перейти за посиланням, що надійшло у повідомленні на Ваш номер телефону смс;

- запитують реквізити Ваших електронних платіжних засобів (карток);

- психологічно тиснуть на особу (погрожують, залякують тощо);

- пропонують скористатися можливістю оформити банківський продукт/послугу в телефонному - режимі.

НАЙЧАСТІШІ ВИПАДКИ ШАХРЙСЬКИХ ДІЙ:

- якщо до Вас надходять підозрілі дзвінки з невідомих мобільних номерів;

- смс-повідомлення сумнівного характеру;

- смс-повідомлення з кодами підтвердження списання коштів з Вашого рахунку;

- повідомлення про реєстрацію або вхід до системи “Клієнт-Банк”;

- повідомлення про участь в “Акціях” та “Розіграшах”, в яких Ви не приймали участь.

У таких випадках необхідно негайно звернутися до відділення Банку, де Ви обслуговуєтесь!

СПІВРОБІТНИКИ БАНКУ НІКОЛИ НЕ ПИТАЮТЬ:

- Строк дії картки;

- Логін чи пароль до будь якого сервісу;

- Дані про телефон (PIN-код, PUK-код);

- PIN-код картки.

- CVV-код картки;

- СМС-коди підтвердження платежів;

- СМС-коди підтвердження входу чи реєстрації в системі “Клієнт Банк”;

БЕЗПЕКА РОЗРАХУНКУ У ПРОСТОРІ ІНТЕРНЕТ

У мережі Інтернет є велика кількість веб-ресурсів, що надають послуги з поповнення мобільних рахунків, переказу коштів тощо.

Будьте обачні, так як деякі з ресурсів можуть використовуватися зловмисниками. На вигляд ці сайти ідентичні реальним, але насправді являються лише копією реальних сайтів.

Персональні дані, що вводяться на таких сайтах (login, пароль, номер картки, CVV2/CVC2-код тощо), потрапляють до рук зловмисників.

ДЛЯ БЕЗПЕКИ РОЗРАХУНКУ У ПРОСТОРІ ІНТЕРНЕТ НЕОБХІДНО ВИКОНУВАТИ НАСТУПНІ ПРАВИЛА

З метою запобігання незаконним діям Держатель Картки при здійсненні розрахунків через Інтернет (а також за телефоном), має дотримуватись деяких рекомендацій:

 Ні в якому разі не використовувати ПІН-код під час замовлення товарів/послуг через Інтернет;

 Не відповідати на електронні листи, у яких від імені банку пропонується надати персональні дані;

 Користуватись послугами тільки відомих і перевірених інтернет-магазинів;

 Здійснювати оплату товарів/послуг тільки зі свого комп'ютера з метою збереження конфіденційності персональних даних та/або інформації про Поточний рахунок;

 Підключитись до послуги Мобільний банкінг. У випадку шахрайства ця послуга надає можливість Держателю Картки своєчасно про це дізнатись і заблокувати картку, зателефонувавши до банку за контактними телефонами.

 Перелік сайтів Банків України можливо знайти на сайті Національного банку України.

 Вводьте персональні дані лише на безпечних сайтах, адреса яких починається з «https://» та мають безпечні сертифікати.

 Не використовуйте одні й ті ж паролі для особистих цілей (для входу на різні сайти мережі Інтернет) та для систем дистанційного обслуговування Клієнтів Банку.

БЕЗПЕКА ВИКОРИСТАННЯ СИСТЕМ ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ КЛІЄНТ-БАНК

Шановні Клієнти АТ «УКРБУДІНВЕСТБАНК»!

Для зменшення ймовірності виникнення незаконних дій з використанням системи Інтернет – банкінгу, будь ласка, ознайомтесь та прийміть до виконання наступні рекомендації:

 Використовуйте актуальні версії операційних систем та програмного забезпечення.

 Використовуйте тільки ліцензійні програмні продукти.

 Використовуйте програмні комплекси для захисту від зловмисного коду (антивірус).

 Не використовуйте комп’ютери, призначені для функціонування системи Інтернет – банкінгу для власний цілей (перегляд листів, використання мережі Інтернет, листування в соціальних мережах тощо).

 Не відкривайте листи сумнівного характеру.

 Будьте обережними з відкриванням вкладень, посилань, інших компонентів сумнівних повідомлень.

 Не використовуйте на комп’ютері, який призначено для користування системою Інтернет – банкінг, змінні носії інформації (флешки), що мають сумнівне походження.

 Якщо використовуються змінні носії інформації (флешки), перед використанням обов’язково необхідно сканувати їх на наявність зловмисного коду (антивірус).

 Використовуйте систему авторизації платежів з використанням СМС повідомлень

ЗВЕРТАЙТЕСЬ ДО БАНКУ НЕГАЙНО В НАСТУПНИХ ВИПАДКАХ

 В разі виникнення сумнівів щодо коректного функціонування комп’ютерного обладнання, своєчасно зверніться до сервісних центрів для обстеження обладнання та повідомте про це представника Банку, де Ви обслуговуєтесь.

 В разі виникнення сумнівів щодо виконання платежів, терміново повідомте Департамент безпеки **АТ «УКРБУДІНВЕСТБАНК»**

 В разі втрати електронного платіжного засобу (картки).

 В разі з’ясування виникнення несанкціонованого доступу або зміні інформації в системах дистанційного обслуговування.

 В разі виявлення фішингових веб-сайтів або отримані відомостей подібного змісту.

 В разі втрати засобів авторизації в системі “Клієнт-Банк”.

Контактні телефони для зв’язку в Банком:

З Банком можна звязатись за телефоном: **(044) 364 34 77 та/або за 0 800 21 97 97**