Як протистояти фішингу?

Шановні Клієнти!

Прискорений розвиток та поширення зручних електронних послуг в мережі Інтернет водночас супроводжується появою нових, все більш хитромудрих способів шахрайства. Банк піклується про безпеку коштів Клієнтів, однак і Клієнти також повинні дотримуватися деяких правил безпеки, які допоможуть не стати жертвами шахраїв.

Одним з найпоширеніших векторів кібератак останній час стало розсилання фішингових електронних листів та фейкових СМС-повідомлень.

Фішинг – будь-які шахрайські дії, спрямовані на крадіжку особистої інформації: паролів інтернет-банкінгу, PIN-кодів, номерів та інших реквізитів платіжних карт, паспортних даних, тощо. Головний інструмент – обман, залучення користувачів на підроблені та фейкові сайти за допомогою фішингових електронних листів, фейкових СМС-повідомлень, переконання у телефонній розмові.

Єдиний спосіб протистояти фішингу – підвищувати рівень обізнаності та відповідальності користувачів, проявляти здорову недовіру до будь-яких вхідних електронних листів та повідомлень, в тому числі до таких, що виглядають як добре відомі або навіть внутрішньо-корпоративні повідомлення.

Загрози поширюються як правило через розсилки електронних листів або переадресування користувачів на підроблені зловмисні веб-сайти. Зловмисники можуть також застосовувати голосовий фішинг, фішингові СМС–повідомлення, фішинг в соціальних мережах, тощо.

Слід знати, що Банк ніколи не запитує в електронних листах, СМС або за телефоном конфіденційну інформацію і в тому числі персональні дані.

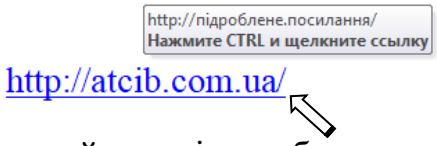
Запам'ятайте: дані, що підтверджують Вашу ідентифікацію для Банку, можуть запитати тільки, коли ВИ самостійно зателефонували до Банку!

Не відповідайте на підозрілі електронні листи, не реєструйтеся на невідомих веб-сайтах, не погоджуйтесь на участь в сумнівних опитуваннях, лотереях, розіграшах, тощо.

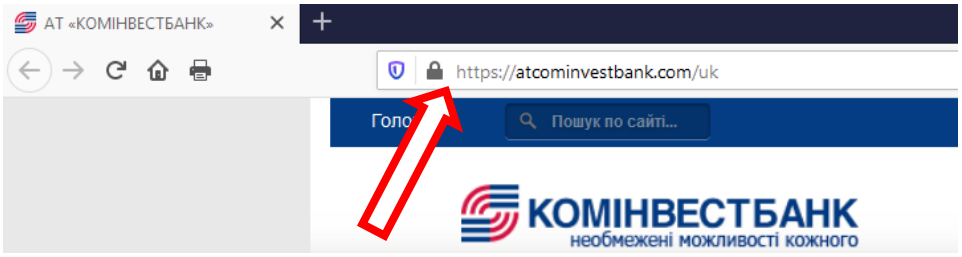
Критично ставтеся до повідомлень про блокування або помилку Вашого аккаунту та необхідність повторного вводу персональної інформації.

Звертайте увагу на граматику отриманого листа або повідомлення, на відповідність до прийнятого стилю спілкування або документообігу з кореспондентом.

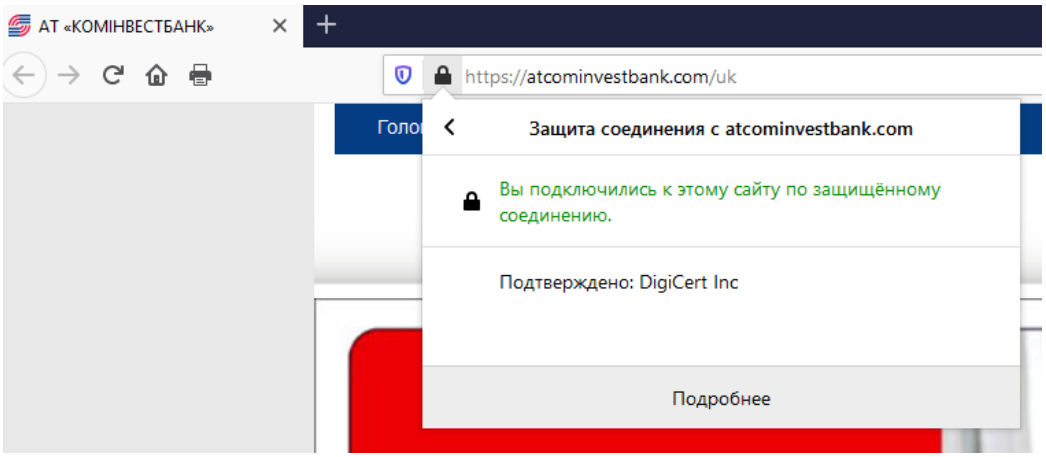
Щоб не потрапити на підроблені зловмисні веб-сайти – не використовуйте посилання у сумнівних листах, завжди перевіряйте, куди веде посилання. Для цього наведіть курсор на посилання і порівняйте адрес в підказці з адресом у посиланні:



Користуйтеся тільки безпечним з'єднанням. Ознакою цього є назва протоколу **https** в адресному рядку та значок закритого замка поруч.



Клік або подвійний клік на значку замка дозволять дізнатися подробиці захисту.



Не відкривайте електронні поштові повідомлення від невідомого або підозрілого кореспондента, ні в якому разі не розпаковуйте в таких повідомленнях прикріплені архіви, не запускайте посилання або виконувані файли.

Складні фішинг-атаки можуть поєднувати лист або СМС з посиланнями на підроблені веб-сайти, вимогу певних дій та пропозицію спілкування та ніби «перевірки ситуації у Банку» за фейковими телефонними номерами. Обов’язково перевіряйте отриману інформацію за телефонними номерами, відомими з незалежного джерела або іншими каналами зв’язку.

У випадку виявлення або підозри фішингу – отримання електронного листа нібито від Банку із запитом конфіденційної інформації, в тому числі персональних даних, виявлення підробленого веб-сайту, що фальсифікує веб-сайт Банку, отримання телефонного дзвінку нібито від фахівця Банку з вимогою надати персональну інформацію рекомендуємо негайно повідомити про це за телефонами, що опубліковані на офіційному веб-сайті Банку:

Приймальна	+38(0312)619804
Відділ супроводження операцій по платіжних картках	+38(0312)669000
Відділ обслуговування фізичних осіб	+38(0312)619811

З повагою,

В.о. Голови Правління
АТ «КОМІНВЕСТБАНК» М.-І.Й. Гатрак