Банк «Pocztowy»

попереджає про методи цифрового шахрайства

Інтернет-банкінг є зручним і надійним способом користування банківськими продуктами. Здійснюючи банківські операції, слід пам'ятати про основні принципи безпеки і усвідомлювати можливу загрозу.

ЯК РОЗПІЗНАТИ СПРОБУ ЦИФРОВОЇ АТАКИ?

СМС

1 ! Якщо Ви отримаєте Смс-повідомлення ніби від Банку, у якому йдеться про:

- зміну особових (напр. номер телефону) даних
- СМС-код для авторизації операції в інтернет-банкінгу

а Ви не здійснювали операції, про які йдеться в Смс-повідомленні

! Якщо Ви помітите на сторінці інтернет-банкінгу, що остання вдала реєстрація відбувалась у момент, коли **Ви не користувались інтернет-банкінгом.**

! Якщо інтернет-браузер вимагає встановлення нових сертифікатів або сторінка інтернет-банкінгу виглядає або поводиться інакше ніж зазвичай, напр. вимагає вказати СМС-код, персональний номер ПЕСЕЛЬ і т.п.

ЯК РЕАГУВАТИ?

Невідкладно з'єднайтесь з Банком і повідомте про тривожні сигнали.

Інформаційна лінія Банку: **тел. 801 100 500 для стаціонарних телефонів, 52 34 99 499 - для мобільних телефонів та стаціонарних телефонів у межах країни та за кордоном.**

Пам'ятайте:

1. **Заблокувати доступ до інтернет-банкінгу**, щоб унеможливити некомпетентним особам доступ до грошових коштів.

2. **Перевити всі останні здійснені операції** на рахунках, а в разі невідповідності, подайте рекламацію.

3. **Видалити шкідливе програмне забезпечення з усіх пристроїв** (комп'ютер/смартфон), найкраще звернутися до IT сервісу. Звичайних антивірусних програм може бути недостатньо.

4. **Видалити збережені дані для реєстрації у транзакційному сервісі** з інтернет-браузерів – якщо Ви користуєтесь збереженням паролів.

5. **Змінити паролі або спосіб входу** на інших пристроях - коли Клієнт користується спареними (напр. Gmail) аккаунами, до яких автоматично входить через смартфон або інтернет-браузер.

ДЖЕРЕЛА ІНФІКУВАННЯ

Шкідливе програмне забезпечення найчастіше зберігається/встановлюється через неуважність, незнання або через те, що хакер підшивався під «довірені» дані або програмне забезпечення. Способів є багато, напр.:

Електронні повідомлення, відправлені на приватні або службові скриньки:

- написане неправильною польською мовою, яке виглядає як перекладене за допомогою комп'ютерної програми
- які обіцяють прибутки, напр., покупку золота за вигідними цінами
- містять вкладення, це можуть бути документи (doc, xls, pdf), архіви (rar, zip), зображення (jpg, png, bmp, git).

Ніколи не відкривайте вкладень від невідомих або сумнівних відправників!

Мобільні додатки:

- які встановлюються з неперевірених сайтів, окрім офіційних (таких, як: GooglePlay або AppStore)
- які встановлюються з сайтів, що імінують повідомлення від антивірусних програм, які повідомляють про «загрозу» і «безкоштовну» можливість сканування пристрою.

Збережені дані для входу:

- ідентичні паролі до різних інтернет-сервісів.
- легкі паролі які не змінювались роками до таких сервісів, як Gmail, який зберігає дуже багато даних доступу (логіни/паролі) і автоматично авторизується в інтернет-браузерах або на смартфорах.

Кожна з ситуацій такого типу може спричинити інфікування пристрою шкідливим програмним забезпеченням, яке здатне:

- **отримувати будь-які дані, які вводяться на клавіатурі пристрою**
- **надсилати стороннім особам знімки екрану пристрою**

- **передавати інформацію про відвідані сайти і дані, введені у них.**
- **передавати інформацію про те, коли пристрій під'єднаний до інтернет-мережі і коли можна активно його використовувати**
- **перехоплювати СМС-повідомлення, що приходять на смартфон**
- **підставляти в інтернет-банкінгу номер рахунку третіх осіб, незважаючи на те, що висвітлюється на екрані.**