

НЕБЕЗПЕКА ВИКОРИСТАННЯ ІНТЕРНЕТ-БАНКІНГУ

Абрамов А. В., ст. (гр. КП-81мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: Зараз існує два найпоширеніші методи шахрайства з платіжними картками – через банкомати та через мережу Інтернет. Тези присвячені проблемам інтернет-банкінгу та способам боротьби з ними.

Ключові слова: Інтернет-банкінг, інформаційна безпека, вразливість, захист даних, безпека даних.

Abstract: Now there are two most common methods of fraudulent payment cards – through ATMs and through the Internet. Abstracts are devoted to problems of Internet banking and ways of dealing with them.

Keywords: Internet banking, information security, vulnerability, data protection, data security.

Інтернет-банкінг – це система віддаленого банківського обслуговування, створена для забезпечення клієнтів максимальним комфортом і зручністю в управлінні фінансами [1]. Основними перевагами даної системи є:

- безкоштовне підключення і відсутність абонентської плати;
- онлайн доступ до банківських рахунків 24/7;
- повний контроль за рухами грошових коштів і залишками на рахунках;
- можливість здійснення банківських операцій у віддаленому режимі, не відвідуючи офіс банку.

Нині Інтернет-банкінг знаходиться на стадії активного розвитку. Проте, до недавнього часу за допомогою Інтернету, можна було просто отримати інформацію про стан рахунку.



На сьогоднішній день Інтернет-банкінг пропонує широкий спектр послуг, а саме: виконувати різноманітні покупки в Інтернеті, виставляти та сплачувати

рахунки, переводити кошти на інші рахунки, оформлювати депозити, отримувати виписки за рахунками, оформлювати заяви на підключення до інших послуг (sms-банкінгу, карток, депозитів, кредитів) і т.п. Більшість клієнтів банків віддають перевагу використанню саме Інтернет-банкінгу, оскільки такий спосіб управління рахунками є зручними і економить час клієнтів.

SMS-банкінг – сучасна послуга, яка дає можливість дистанційно скористатись банківськими послугами, мати доступ до рахунків та операцій за рахунками 24 години на добу з номеру мобільного телефону, який закріплено за користувачем у банку. Для виконання операцій використовуються SMS повідомлення. Таким чином необхідність встановлення додаткового програмного забезпечення на мобільний телефон (зокрема JAVA програми) відсутня.

Розглядаючи розвинені країни світу, можна зробити висновок, що в них Інтернет-банкінг став швидко популярним серед фізичних осіб та власників малого бізнесу. За оцінками ЮНКТАД (Конференція Організації Об'єднаних Націй з торгівлі та розвитку), в Західній Європі кількість користувачів Інтернет-банкінгу зростатиме на 20% щороку. За даними досліджень «com Score», в США 66% американських споживачів сплачують рахунки через мережу Інтернет [2].

Основна загроза при використанні Інтернет-банкінгу полягає в тому, що шахраї можуть зламати рахунок користувача та отримати доступ до його коштів. У зв'язку з цим, банки використовують різноманітні системи та механізми для підвищення безпеки при використанні Інтернет-банкінгу та уникнення ситуацій злову рахунків [3].

Найбільш відомий спосіб шахрайства – перехоплення ідентифікаційних даних і ключів для електронного підпису користувача. Зробити це можна двома способами: за допомогою зараження комп'ютера користувача спеціальними вірусами та за допомогою схеми «men in the middle». Суть цієї схеми полягає в тому, що шахраї перехоплюють дані, як тільки користувач надіслав свої дані до банку. Зловмисники мають змогу змінити ці дані і потім відправити їх до банку. Така ситуація можлива, коли канал передачі даних не зашифрований.

Найбільш поширеними системами забезпечення безпеки є: шифрування каналів для передачі даних та ідентифікація користувачів зв допомогою криптографії та електронного цифрового підпису. Для більшої надійності краще комбінувати ці способи.

Якщо при роботі з Інтернет-банкінгом не використовуються системи електронного підпису або генератора пароля, то клієнт може стати жертвою зловмисників.

Користувачам Інтернет-банкінгу варто приділяти увагу не лише наявності системи електронного підпису, а й слідкувати за оновленнями антивірусного та системного ПЗ на своїх комп'ютерах.

Розглянемо основні способи захисту від інтернет-шахрайств.

1. Користувач має підключити собі смс-інформування. Тобто при розрахунку картою, платник отримуватиме повідомлення на свій мобільний телефон про транзакцію. Зазвичай, таку послугу користувачі можуть замовити при отриманні картки або звернувшись до сервісного центру банку.

2. Управляти лімітами за платіжною картою. Наприклад, можна встановити певний ліміт на розрахунки в Інтернеті на добу. Якщо необхідно здійснити більшу транзакцію – то є можливість збільшити ліміт. Після успішної транзакції, ліміт можна зменшити до мінімуму, і таким чином, вберегти свої кошти від їх використання шахраями в мережі Інтернет.

3. Необхідно не допускати передачу своїх мобільних телефонів, які підключені до банківської картки, незнайомим особам.

4. Не розголошувати свої логін та пароль до інтернет-банкінгу, пін-код картки та CVV-код. Навіть працівники банку не мають доступу до цієї інформації, отже не треба звертати увагу на дзвінки та повідомлення з проханням надати подібну інформацію.

5. Для кращого захисту, клієнтам Інтернет-банкінгу не варто залишати номер мобільного телефону, який прив'язаний до банківської карти у відкритому доступі.

6. Варто регулярно міняти пароль від Інтернет-банкінгу, не рідше, ніж раз на півроку. Для того, щоб мати складний пароль, можна скористатись спеціальними системами для генерування та збереження паролів [4].

Висновок. Сьогодення вносить свої корективи в повсякденне життя. Тому не дивлячись на всі ризики, що пов'язані з використанням Інтернет-банкінгу переваг все ж таки більше. Єдине користувачам треба дотримуватись правил безпеки.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КНІ ім. Ігоря Сікорського)

Література

1. Інтернет-банкінг [Електронний ресурс]. – Режим доступу: <https://uk.wikipedia.org/wiki/Інтернет-банкінг>.

2. Огієнко В. І., Луняков О. В. Інтернет-банкінг як перспективний напрям розвитку ринку фінансових послуг [Електронний ресурс]. – Режим доступу: <http://www.economy.nayka.com.ua/?op%20=1&z=1217>.

3. Безпека Інтернет-банкінгу: практичні аспекти [Електронний ресурс]. – Режим доступу: http://www.bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_praktichni_aspekti.

4. Найпоширеніші шахрайства з банківськими картками: як не попастися [Електронний ресурс]. – Режим доступу:

http://tvoemisto.tv/news/nayposhyrenishi_shahraystva_z_bankivskymy_kartkamy_yak_ne_popastysya_82728.html.