Рекомендації клієнтам АТ «АБ «РАДАБАНК» щодо виявлення фішингових вебсайтів та посилання на сторінку офіційного Інтернет-представництва Національного банку, на якій розміщено перелік власних вебсайтів банків

1. Що таке фішинг?

Фішинг – це певна схема, застосування якої змушує користувачів передавати певну конфіденційну інформацію для послідуючого використання такої інформації у зловмисних цілях. До такої інформації відносяться: логіни та паролі, номера, термін дії та інші реквізити платіжних карток, адреса електронної пошти та номера фінансових телефонів, відповіді на секретні питання, тощо.

Схема як правило працює у двох напрямках – використання несанкціонованих розсилок електронних листів (СПАМу) та переадресування користувачів на зловмисні (підробні) вебсайти які ззовні або по імені дуже схожі на офіційні вебсайти певних організацій. Зловмисниками можуть також застосовуватись голосовий фішинг, фішингові СМС-повідомлення та фішинг в соціальних мережах, але по принципу дії вони дуже схожі, тому на них зупинятись ми не будемо.

Суть використання схеми з фішинговими вебсайтами – збір конфіденційної інформації. Тобто при виконанні певних дій зі сторони користувача операції (як то відправка інформації з певних форм чи здійснення транзакції по платіжній картці) фактично не виконуються, а введена користувачем інформація – направляється злочинцям для використання у зловмисних цілях. Як приклад, отримавши по схемі фішинга інформацію про номер платіжної картки, термін дії, імені та прізвище власника платіжної карти, CVV-коду – зловмисники використовують цю інформацію для здійснення несанкціонованих списань грошових коштів з таких платіжних карт. Користувач дізнається про такі несанкціоновані операції вже по факту їх здійснення, отримуючи інформацію про рух коштів за допомогою СМС-банкінгу чи перегляду руху коштів в системах дистанційного обслуговування рахунків.

З більш розширеною та детальною інформацією про фішинг можна ознайомитись на офіційному вебсайті провідного розробника програмних продуктів для захисту від зловмисного коду – компанії ESET: https://eset.ua/ua/support/entsiklopediya_ugroz/fishing

2. Як розпізнати фішинговий вебсайт?

Щоб зберегти свої персональні дані (конфіденційну інформацію) та грошові кошти в безпеці перед тим як вводити свої дані на вебсайті потрібно звернути увагу на:

2.1. Неправильне доменне ім'я – як правило, шахраї реєструють схожі домени. Наприклад, замість «radabank.com.ua» можна побачити «rada.bank.com.ua» або «radbank.com.ua». Також сайт може розташовуватися на піддомені, наприклад, «radabank.site.ua» тощо.

2.2. Відсутність SSL сертифікату – пошукові системи використовують шифрування SSL для передачі даних користувачів. При використанні цієї технології адреса сайту починається на «https: //». Якщо вебсайт починається на «http: //», це привід засумніватися в оригінальності сторінки. Шахраям не важко отримати дійсний SSL сертифікат для підробленого сайту – його можна отримати безкоштовно за допомогою спеціальних сервісів.

2.3. Граматичні, орфографічні і дизайнерські помилки – розпізнати шахраїв можна за наявністю граматичних і орфографічних помилок в тексті вебсайтів. Насторожити повинні неправильні назви організації, велика кількість помилок. Наприклад, збилась верстка, неправильне використання кольорів в дизайні, наявність сторонніх елементів дизайну.

2.4. Різниця структур сторінок з оригінальним сайтом і підозрілі платіжні форми – потрібно звертати увагу на наявність посилань на сторінці. Якщо при натисканні на них ви переходите на сторінку з помилкою або на сторінки, які не схожі на оригінальний вебсайт, значить, ви потрапили на фішинговий сайт. Просто закрийте вкладку і не вводьте персональні дані в платіжні форми.

2.5. Старий дизайн – ознакою фішингової форми може стати той факт, що вона розміщена на тлі застарілого дизайну вебсайту. Якщо вебсайт викликав у вас підозру, ігноруйте його та платіжну форму.

2.6. Розділ вебсайту «Контакти» – слід перевіряти розділ «Контакти», щоб переконатись, що фізична адреса вказана правильна, а не вигадана. Наприклад, авіакомпанія не може перебувати в промисловій зоні, а банківська установа в покинутому офісі на околиці міста.

При роботі з електронною поштою все набагато простіше – жодна банківська установа не буде розсилати електронні повідомлення як своїм діючим так і потенційним клієнтам, в яких буде міститись посилання на якісь вебсайти для здійснення фінансових операцій. Всі фінансові операції, окрім розрахунків з використанням особистих кабінетів інтернет-магазинів, чи сервісів замовлення квитків, здійснюються виключно через системи дистанційного обслуговування рахунків (тобто клієнт-банк). Таким чином отримавши електронне повідомлення на свою пошту з проханням чи пропозицією перейти за посиланням та здійснити передачу своїх облікових даних чи здійснити операцію з платіжною карткою – можете бути впевненими, що це на 99,99% несанкціонована шахрайська розсилка.

3. На що звертати увагу при роботі з вебсайтами АТ «АБ «РАДАБАНК»?

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб при роботі з вебсайтами Банку для клієнтів Банку розроблено ряд рекомендацій наведених нижче:

3.1. Запам’ятайте та завжди використовуйте при роботі з вебсайтами інформацію наведену в розділі2 даних Рекомендацій;

3.2. Завжди здійснюйте візуальну перевірку перевіряти доменне ім’я для впевненості, що це офіційна, а не фішингова сторінка зловмисників. На даний час АТ «АБ «РАДАБАНК» має наступні офіційні вебсайти:

https://www.radabank.com.ua/ – офіційний корпоративний вебсайт Банку в мережі Інтернет;

https://coinsshop.radabank.com.ua/ua/shop/ – офіційний вебсайт Банку «Магазин монет»;

https://ibank.radabank.com.ua:4443/web/ – офіційний вебсайт Банку для доступу до системи дистанційного обслуговування «Веб-банкінг для корпоративних клієнтів», призначений для використання клієнтами Банку – юридичними особами;

https://ib.radabank.com.ua/ib2/ офіційний вебсайт Банку для доступу до системи дистанційного обслуговування «RB24», призначений для використання клієнтами Банку – фізичними особами.

3.3. Виконуйте перевірку кому та ким виданий SSL сертифікат і стежити за строком його дії (Рис.1). Натиснувши на значок «замка» ліворуч від доменого імені (Рис.2) можна переглянути властивості сертифікату:

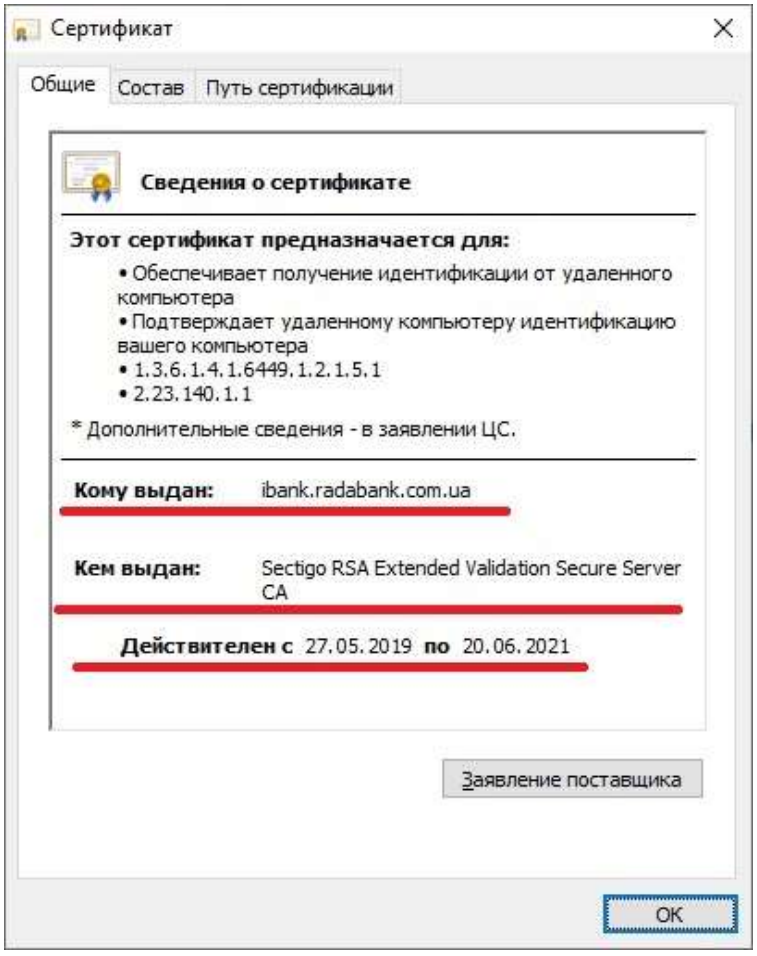

Рис.1

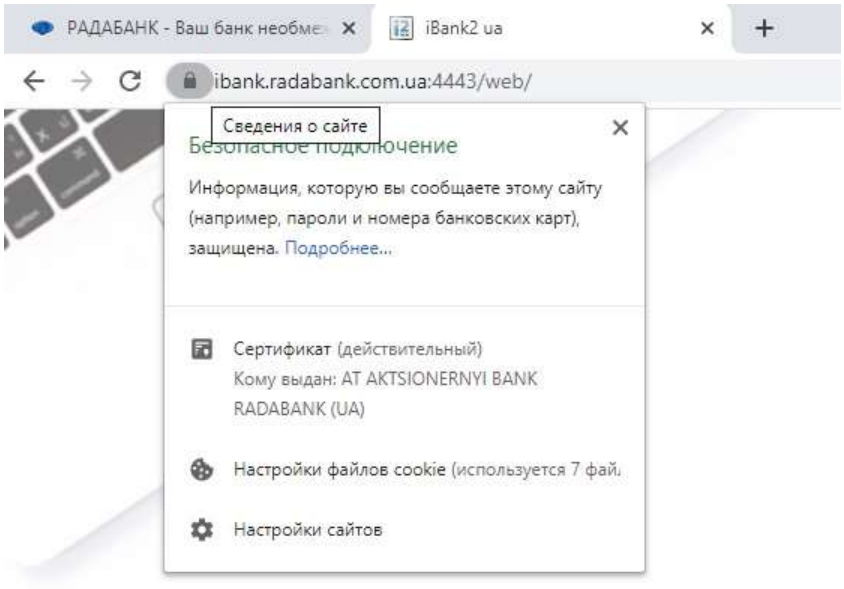

Рис.2

Зображення замкнутого «замка» означає, що на вебсайті встановлений SSL-сертифікат і вся інформація передається по захищеному протоколу. SSL-сертифікат не дає шахраям перехопити або підмінити особисті дані користувачів.

3.4. Ніколи не здійснюйте введення конфіденційної інформації у разі якщо Вас було переадресовано на невідомий вебсайт з незрозумілим доменним іменем. Використовуйте виключно офіційні доменні імена АТ «АБ «РАДАБАНК» чітко визначені в підпункті 3.2. даних рекомендацій.

3.5. Повторно наголошуємо, що АТ «АБ «РАДАБАНК» ні при яких обставинах не здійснює телефонні дзвінки свої діючим та потенційним клієнтам для отримання будь-якої конфіденційної інформації. Отримання конфіденційної інформації виконується виключно у разі особистої присутності клієнта у приміщеннях Банку (в Головному офісі чи відділеннях Банку) та з використанням систем дистанційного обслуговування рахунків Банку.

3.6. За необхідності для впевненості, що Ви знаходитесь на вебсайті потрібної Вам фінансової установи, можна скористатись офіційним переліком власних вебсайтів банків України розташованому на сторінці офіційного Інтернет-представництва Національного банку України.

4. Перелік власних вебсайтів банків України.

Для унеможливлення потрапляння клієнтів банків на фішингові вебсайти Національний банк України на своєму офіційному Інтернет-представництві розмістив офіційний перевірений перелік вебсайтів банків України. Перейшовши за даним посиланням можна легко перевірити автентичність доменного імені та належність вебсайту конкретній банківській установі:

https://bank.gov.ua/supervision/institutions