Рекомендації щодо захисту від фішингу

Що таке фішинг?

Фішинг (англ. Phishing, від fishing - риболовля, видобування) - вид інтернет-шахрайства, з метою отримання доступу до конфіденційної інформації користувачів (логінів і паролів). Це досягається шляхом проведення масових розсилок електронних листів або повідомлень всередині соціальних мереж від імені популярних компаній в т.ч. і від імені банків. У листі часто міститься пряме посилання на сайт, який зовні не відрізнити від справжнього. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленої сторінці свої логін і пароль, які він використовує для доступу до певного сайту, що дозволяє шахраям отримати доступ до облікових записів і банківським рахунках користувача.

Ознаки фішингових листів:

Адреса відправника

Електронна адреса, що відображається в полі "Від", НЕ є гарантією відправки електронного листа через поштову систему ПАТ "МТБ Банк". Фішингові повідомлення зазвичай мають вигляд електронного листа, зовні невідмітного від оригінального, відправленого з поштової системи ПАТ "МТБ Банк". За допомогою шкідливого програмного забезпечення, зловмисники можуть підмінити електронну адресу джерела, який відображається в будь-якому поштовому клієнті.

2. Екстрений характер повідомлення

Для збільшення числа відгуків зловмисники намагаються надати повідомленню екстрений характер, позначити ліміт часу, тим самим викликаючи негайну, необдуману реакцію одержувача.

3. Помилки в темі листа

У фішингових листах, як правило, в поле "Тема:" з метою обходу фільтрів поштових програм, використовується різний регістр букв, набір букв і цифр, граматичні помилки або друкарські помилки (Наприклад: помилка, о111ібка).

4. Гіперпосилання на підроблені сайти

Посилання в фішингових повідомленнях, зовні не відрізняються або є мало відмітними від офіційної веб адреси ПАТ "МТБ Банк", перенаправляють користувачів на веб-сайти, що імітують вид легітимного сайту Банку.

Як розпізнати підроблений сайт?

1. Адреса веб-сайту

Більшість методів фішингу зводиться до того, щоб замаскувати підроблені посилання на фішингові сайти під посилання справжніх організацій. Адреси з помилками або субдомени часто використовуються шахраями. Насправді адреса сайту (URL), якій зовні не відрізнити від офіційної адреси банку, складається з набору цифр і букв і вміст сайту є підробленим.

Проте, частина відображаємої інформації і некритичні посилання можуть бути оригінальними.

2. Спливаючі вікна

За допомогою різного шкідливого програмного забезпечення зловмисники можуть розміщувати

спливаючі підроблені вікна на підставі легітимного сайту, які запитують конфіденційну інформацію. При цьому справжній сайт Банку буде відображатися в фоновому режимі. Таким чином, вся вводимо Вами інформація в підробленому спливаючому вікні буде доступна шахраям.

Як захиститися від фішингових атак?

ПАТ "МТБ Банк", ніколи не запитує у клієнтів конфіденційну інформацію по електронній пошті, не здійснює розсилку листів з проханням прислати секретний ключ ЕЦП або пароль, не розсилає програмне забезпечення для установки на Ваші комп'ютери.

Дотримання перерахованих нижче правил дозволить Вам успішно протистояти фішингових атак:

1. Ніколи не надавайте секретний ключ Електронного цифрового підпису (ЕЦП), пароль або інші конфіденційні дані стороннім особам. Ніколи не відповідайте на електронні листи, в яких запитується Ваша персональна або фінансова інформація і не переходите по зазначеним в них посиланнях, так як всі листи, що запитують персональні дані, є шахрайськими.

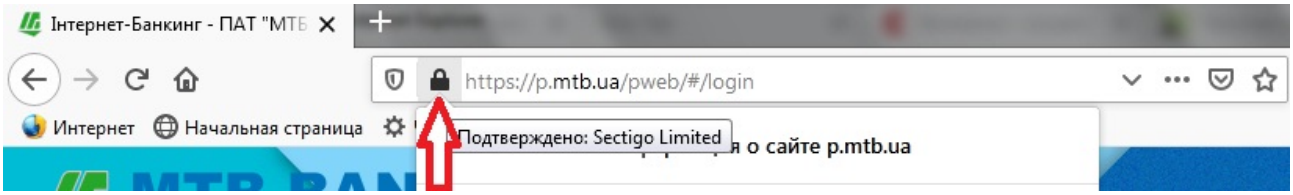
2. Якщо Ви отримали підозрілий електронний лист від імені ПАТ "МТБ Банк", зв'яжіться з цілодобової Інформаційно-довідкової службою ПАТ "МТБ Банк", за телефонами 0 800 500-255 або +38(0482) 305-905 (всі дзвінки зі стаціонарних телефонів на території України безкоштовні), або перешліть підозрілий лист з коментарями на адресу: office@mtb.ua

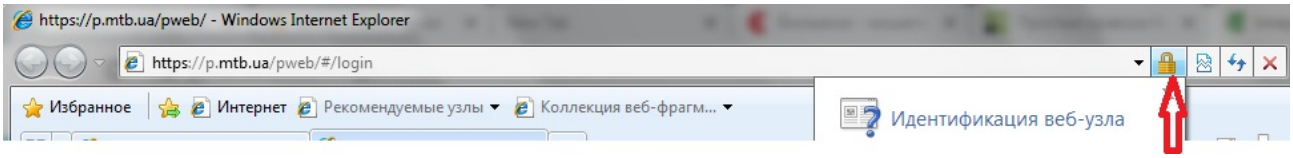
3. Для входу на веб-сторінку Інтернет банкінгу ПАТ "МТБ Банк" використовуйте виключно адресу https://p.mtb.ua/pweb/#/login (Для фізичних осіб) та https://i.mtb.ua/web/ (Для юридичних осіб та ФОП), набраний ВРУЧНУ в адресному рядку Вашого браузера або користуйтеся власними закладками.

4. Завжди перевіряйте, що для передачі персональної інформації використовується шифроване з'єднання. Адреса сайту завжди починається з "https: //", а не з http: // в разі, якщо використовується безпечне з'єднання.

5. Для підтвердження автентичності сайту Інтернет банкінгу ПАТ "МТБ Банк" , необхідно перевірити цифровий сертифікат безпеки шляхом натискання на символ безпечного з'єднання в Вашому браузере (Символ безпечного з'єднання індивідуальний для кожного браузера.), як зазначено на малюнку:


p.mtb.ua/pweb/#/login
Apps
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.


Інтернет-Банкинг - ПАТ "МТБ
https://p.mtb.ua/pweb/#/login
Интернет
Начальная страница
Подтверждено: Sectigo Limited
о сайте p.mtb.ua


https://p.mtb.ua/pweb/ - Windows Internet Explorer
https://p.mtb.ua/pweb/#/login
Избранное
Интернет
Рекомендуемые узлы
Коллекция веб-фрагм...
Идентификация веб-узла