Кодекс безпеки

mBank

mBank.pl

Зміст

У Кодексі безпеки знайдеш поради щодо того, як безпечно користуватися онлайн та мобільним банкінгом, а також як захиститися від загроз з боку кіберзлочинців.

Пристрій 

1. Користуйся послугами банку тільки на перевірених пристроях. Уникай входу з чужих комп'ютерів та мобільних пристроїв.
2. Використовуй додаткові програми (антивірус чи брандмауер), які захищають комп'ютери та мобільні пристрої.
3. Регулярно оновлюй операційну систему на своєму комп'ютері.
4. Не змінюй конфігурацію безпеки пристрою самостійно, і зокрема не знімай обмежень, встановлених виробником.
5. Завантажуй додатки та програми лише з офіційних джерел.
6. Увімкни налаштування блокування екрана свого пристрою (це може бути пароль чи PIN-код).

Паролі 

1. Використовуй складні паролі. Зроби їх важкими для вгадування (мінімум вісім символів, включаючи спеціальні символи, цифри, великі та малі літери).
2. Не використовуй тривіальні фрази у своєму паролі та інформацію, яку легко зв'язати з тобою (наприклад, ім'я чи прізвище) або вгадати (наприклад, поточний місяць, рік).
3. Регулярно змінюй свої паролі і нікому не повідомляй їх.
4. Використовуй унікальні паролі для послуг банку. Не використовуй паролі, які ти використовуєш в інших банківських системах, на форумах чи порталах.

Сторінки www 

1. Перевіряй правильність веб-сайту банківської служби, до якої ти підключаєшся (сертифікат та HTTPS-з'єднання).
2. Не відвідуй підозрілі та невідомі сайти – звертай увагу на URL-адреси сторінок, які ти відвідуєш, особливо на так звані скорочені URL-адреси, наприклад http://bit.ly/2GeFeLg. Такі веб-сайти можуть заразити твій пристрій шкідливим програмним забезпеченням.
3. Не надавай персональні дані на ненадійних веб-сайтах, зокрема ніколи не повідомляй логін та пароль свого банку на веб-сайтах інших сайтів.
4. Під час входу на веб-сайти банку або платіжного інтегратора завжди вводь сторінку входу самостійно або використовуй кнопку «Увійти» після ручного введення адреси веб-сайту. Ніколи:
   - не використовуй посилання для входу, які ти отримуєш на електронну пошту чи в соціальних мережах
   - не шукай сторінку входу в пошуковій системі – ти можеш натрапити на підроблені сторінки, які видають себе за веб-сайт вашого банку.

Електронні листи

1. Не відкривай підозрілі повідомлення електронної пошти та прикріплені файли.
2. Зверни особливу увагу на прикріплені файли з кількома розширеннями одночасно, наприклад transfer.pdf.zip, wyplata.jar.doc.
3. Перевір, чи справжня адреса посилання (лінк) відповідає тій, яку ти бачиш в тілі електронного листа (перевір це, перемістивши курсор на посилання та виділивши адресу).
4. Зверни увагу на достовірність відправника та на те, як він до тебе звертається.
5. Ніколи не входь до сервісу транзакцій за посиланням, яке ти отримав в електронному листі.
6. Не здійснюй транзакцій на основі електронної пошти. Уважно перевір ці типи інструкцій.

Портали та інтернет-пропозиції

- Якщо ти отримав від друга прохання зробити для нього/неї переказ, будь обережним – можливо, ти спілкуєшся з шахраєм. Зв'яжись зі своїм другом іншим способом і підтверди, що він насправді просить тебе про грошовий переказ.
- Перед покупкою уточнюй, у кого ти купуєш товар: скільки років існує компанія, де вона знаходиться, чи можна зателефонувати на гарячу лінію магазину, чи відповідають вони на електронні листи та яку думку висловили інші покупці. Переконайся, що ти можеш оплатити через інтегратор платежів.
- Не довіряй пропозиціям про роботу, які ти отримав прямо на свою почтову скриньку, особливо дуже «привабливим». Не піддавайся на пропозиції фінансових брокерів, які можуть виявитися злочинними. При пошуку роботи користуис я тільки відомими порталами.

Телефонні розмови

1. Не розкривай особисту інформацію, поки не впевнений можеш перевірити співробітника банку, передзвонивши на mLine і підтвердити и
2. Не довіряй невідомому абоненту, який хоче, щоб ти повідомив конфіденційні дані (зокрема паролі, номери платіжних карток, PIN-коди), наприклад, під приводом:

- розслідування злочинної групи (так званий метод «поліцейського») або
- перевірка рахунку, підтвердження переказу або повернення коштів (так званий метод «співробітника банку»).

Поліцейський або банківський працівник ніколи не попросить у тебе конфіденційні дані (наприклад, пароль, PIN-код додатку чи картки) твого облікового запису.

Картки

1. Перш ніж використовувати банкомат, перевір його на наявність дивних планок, накладок або контейнерів для брошур. Додатково подивись на вхід зчитувача, куди ти вставляєш картку – злочинці можуть розмістити так звані шумівки, або накладки які «зчитують» картки. Клавіатура пристрою повинна бути плоскою, без чітко виступаючих елементів.

2. Під час введення PIN-коду обов'язково прикривай клавіатуру іншою рукою (якщо злочинець встановив мікрокамеру, звернену до клавіатури).
3. Якщо тебе щось турбує, припини транзакцію і спокійно відійди від пристрою. Потім повідом власника банкомату (номер телефону є на кожному пристрої).
4. При оплаті в торговій точці ні за яких обставин не втрачай картку з поля зору (навіть якщо ти знаєш і любиш даний ресторан). Співробітник повинен підійти до тебе з терміналом.
5. Оплачуючи карткою онлайн, переконайтеся, що:
   - підключення до сайту безпечне – адреса веб-сайту починається з https://
   - адреса введена вірно
   - веб-сайт має дійсний сертифікат (у верхньому вікні браузера має бути маленький значок із замком).

Повідомлення 

1. Уважно читай повідомлення мобільної авторизації та SMS- повідомлення. Деталі операції (тип операції, номер рахунку та сума), отримані в повідомленні про авторизацію або SMS, повинні відповідати тому, що ти замовив в сервісі транзакцій.
2. Уважно читай попередження mBank про нові загрози та дотримуйся рекомендацій.
3. Якщо ти отримав повідомлення від оператора зв'язку про видачу дубліката SIM-карти, яку ти не замовляв, негайно зателефонуй консультанту mLinia або онлайн-експерту.

Послуги 

1. Використовуй мобільну авторизацію – новий безпечний метод підтвердження транзакцій, заснований на мобільному додатку mBank.
2. Увімкни зашифровані виписки – послуга mBank з доставки зашифрованих виписок, завдяки якій інформація, що міститься у твоєму рахунку та виписках з кредитної картки, стане ще безпечнішою.

Пам'ятай! 

Дані сьогодні – тверда валюта. Прості атаки соціальної інженерії можуть призвести до того, що кіберзлочинці виведуть гроші з твого рахунку. Увімкни шифрування виписок, використовуй надійні паролі не тільки для банківських операцій, а й для всіх веб-сайтів, де зберігаються твої дані. Перш ніж вводити свої дані у форму, подумай, як ти сюди потрапив і який обсяг даних ти маєш надати.

Можливо, ти перебуваєш на сайті, підготовленому злочинцями. Якщо будь- яке повідомлення, комунікат або елемент транзакційного чи мобільного сервісу викликають у тебе сумніви – припини активність і негайно зателефонуй консультанту mLinia чи онлайн-експерту.