03
IV КВАРТАЛ
2024 РОКУ
Наступну газету можна отримати у сервісному центрі Пенсійного фонду України

Фінансова мудрість

Безкоштовна соціальна газета з фінансової грамотності для людей старшого віку від Національного банку України, АБ КБ "ПриватБанк" та БО "БФ "Життєлюб"

Національний банк України
ПриватБанк
Життєлюб
Благодійний фонд

"Сьогоднішня моя розповідь не про кохання, а про щось набагато прозаїчніше – як захистити свої гроші від шахраїв"

П'ять порад

від українського актора театру та кіно
Олексія Вертинського

Надійний пароль – це як замок, який захищає Ваш будинок від злодіїв

Уявіть, що Ваш дім – фортеця, наповнена цінними для Вас речами. Ви ж не замикаєте її двері на простий замок-гачок? Чи не так? Ваш смартфон, платіжна картка, сторінки в соціальних мережах теж мають свої цифрові замки. Якщо використовувати легкий пароль, наприклад, ім'я Вашої дитини або дату її народження, він буде передбачуваним для шахрая. Щоб зробити пароль надійним, використайте улюблену цитату та додайте кілька цифр, крапок, ком чи тире.

Продовження на 6-й стор.

Надійний пароль – ключ до захисту Ваших даних в інтернеті!

Дотримуйтеся простих і ефективних способів створення та зберігання паролів, які допоможуть убезпечити Ваші дані від зловмисників в інтернеті.

1. Створюйте надійні паролі до всіх сервісів і пристроїв, які Ви використовуєте.

Маються на увазі паролі до інтернет-банкінгу, сторінок у соціальних мережах, месенджерах, онлайн-кабінетів будь-яких сайтів, електронної пошти, смартфона тощо.

Надійним паролем вважається складний та унікальний пароль.

Складний пароль повинен містити:

- щонайменше 12 символів;
- великі та малі літери;
- цифри, спеціальні знаки та символи, наприклад: !@#$%^&* (навіть пробіли).

2. Уникайте паролів, які можна легко вгадати.

Під час створення пароля не використовуйте:

- **особисту інформацію** Вашу чи Ваших близьких: дітей, онуків, друзів тощо. Це означає, що не слід використовувати дату народження, прізвище, ім'я, адресу, номер телефону, дівоче прізвище та навіть ім'я Вашого домашнього улюбленця;
- **загальновідомі комбінації паролів** (наприклад, Password123456, Admin1234 тощо);
- **послідовне або зворотне написання символів або цифр** на клавіатурі комп'ютера чи смартфона (наприклад, Qwerty12334 тощо).

3. Придумайте пароль, який запам'ятати просто, а вгадати неможливо.

Для цього використовуйте фрази – кодові слова. Наприклад, для створення пароля можна поєднати смак улюбленого печива, рік, коли Ви придбали власне житло, додати спеціальні символи. В результаті може вийти така комбінація для пароля: **Smak_Kokos1982%.**

4. Використовуйте різні паролі.

Однакові паролі – це те саме, що мати один ключ до будинку, автомобіля, сейфа. Якщо зловмисники отримають доступ до цього пароля, вони зможуть отримати доступ до всіх сервісів, де він використовується.

5. Надійно зберігайте паролі.

- Не діліться паролями через електронну пошту або повідомлення.
- **Запам'ятовуйте паролі! Це – найнадійніший спосіб їх зберігання.**

Якщо Ви прийняли рішення записати Ваші паролі на папері, подбайте, щоб ці записи зберігалися в надійному місці.

6. Не вводьте паролі на невідомих та підозрілих сайтах.

Остерігайтеся шахрайських сайтів та посилань в інтернеті

Зловмисники з метою отримання конфіденційної інформації про паролі, платіжні картки, рахунки та інших особистих даних:

- створюють сайти, схожі на офіційні сайти державних, міжнародних, банківських та інших установ;
- поширюють в інтернеті шахрайські посилання;
- надсилають електронні листи або повідомлення, які можуть містити шахрайські посилання та заражені вірусами файли.

Перевіряйте сайти, на яких вводите свої дані

Навіть якщо сайт, на який Ви перейшли, виглядає знайомим, **зверніть увагу, чи є такі ознаки шахрайських сайтів:**

- помилки в тексті, перекладений текст за допомогою машинного перекладу;
- недостатність контактної інформації про компанію або її власника;
- не всі сторінки сайту заповнені інформацією;
- немає угоди користувача / розділу політики конфіденційності (приватності).

Якщо Ви не впевнені у справжності сайту, попросіть про допомогу у своїх близьких та родичів.

ВАЖЛИВО! Якщо потрібно перейти на сайт компанії, адресу якого Ви отримали в повідомленні чи побачили в інтернеті, краще введіть у Google назву потрібного сайту і лише потім переходьте на сайт.

Перевіряйте посилання, на які натискаєте!

Не переходьте за посиланнями від незнайомців!

Шахраї поширюють шкідливі посилання в месенджерах, смс-повідомленнях, групових чатах, соціальних мережах, електронною поштою; розміщують рекламу в інтернеті тощо, щоб дізнатися інформацію про Ваші картки, рахунки або інші персональні дані.

Якщо отримали посилання від знайомого, не поспішайте на нього натискати

Шахраї могли отримати доступ до його сторінки в соціальних мережах, електронної пошти тощо. **Запитайте в знайомого, для чого він надіслав посилання,** або краще зателефонуйте йому та запитайте, чи справді посилання від нього. Прикладами таких посилань можуть бути такі: "Подивіться, чи це Ви на відео?" або "Перейдіть за посиланням та виграйте мільйон" тощо.

Що робити, якщо Ви повідомили зловмисникам зайву інформацію?

Якщо Ви випадково розкрили дані своєї платіжної картки, інтернет-банкінгу на підозрілому сайті, **негайно телефонуйте до банку за номером, зазначеним на звороті картки.**

Банківський застосунок у Вашому смартфоні

Сучасні банківські застосунки створені для зручності та надають безліч можливостей своїм користувачам. Майже кожен український банк розробив свій офіційний застосунок, завдяки якому Ви можете не ходити до відділення, а за кілька хвилин здійснити безліч операцій зі свого смартфона.

Ось як можна швидко і легко встановити банківський застосунок на свій смартфон:

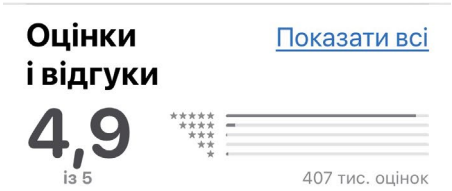
1 Вибір застосунку.

Спочатку визначте, який банківський застосунок Вам потрібен. Переконайтеся, що це офіційний застосунок Вашого банку. **Для цього:**

- **перевірте назву розробника:** використовуйте **Google Play Market** або **App Store** та зверніть увагу на назву розробника – вона має збігатися з назвою Вашого банку;

- **відвідайте офіційний сайт банку:** часто банки надають посилання на свої застосунки на своєму офіційному сайті;

- **перевірте відгуки та рейтинг:** офіційні застосунки зазвичай мають велику кількість відгуків та високий рейтинг;



- **перевірте кількість завантажень:** офіційні застосунки великих банків мають мільйони завантажень, менші банки – десятки та сотні тисяч. Це також може бути додатковим підтвердженням автентичності застосунку.

2 Завантаження.

- **Для користувачів Android** відкрийте Google Play Market.
- **Для користувачів iOS** відкрийте App Store.

У рядку пошуку введіть назву банку або назву його застосунку. Натисніть "Завантажити" або "Встановити".

1 **Не користуйтеся загальнодоступними мережами Wi-Fi** – це Wi-Fi, до якого можна підключатися без необхідності введення пароля (зазвичай доступний у громадських місцях).

Такі мережі не захищені належним чином, що дає змогу шахраям перехоплювати дані банківських карток, паролі, повідомлення та інші конфіденційні дані.

2 **Вигадайте унікальний та складний пароль** для входу в застосунок, який знаєте лише Ви. Про те, як створити надійний пароль, читайте на стор. 2.

3 Стежте за тим, щоб на Вашому мобільному телефоні чи комп'ютері було встановлено та своєчасно оновлювалось **антивірусне програмне забезпечення.**

3 Встановлення.

Після завантаження натисніть "Відкрити", щоб розпочати процес встановлення. Дотримуйтесь інструкцій на екрані, які можуть включати надання дозволів застосунку для доступу до певних функцій Вашого смартфона (контакти, повідомлення тощо).

4 Реєстрація.

Після встановлення Вам потрібно буде зареєструватися або увійти у свій обліковий запис. Зазвичай це вимагає введення номера телефону або електронної пошти, а також створення пароля. Деякі банки можуть також попросити підтвердити Вашу особу за допомогою одноразового пароля (OTP), який буде надіслано на Ваш смартфон.

5 Налаштування безпеки.

Щоб забезпечити безпеку Вашого облікового запису, активуйте функції безпеки, такі як біометрична автентифікація (відбиток пальця або розпізнавання обличчя) або двофакторна автентифікація.

Які переваги використання таких технологій?

- Швидкість та надійність.
- Стійкість до компрометації (підробки).
- Не потрібно запам'ятовувати складні паролі.
- Вищий рівень конфіденційності.

Безпечне використання банківського рахунку

- **Ніколи не надавайте інформацію про свої платіжні картки третім особам,** навіть якщо вони звертаються до Вас начебто від імені банку чи служби безпеки банку, Національного банку України, Пенсійного фонду України, поліції.
  Банки не телефонують та не надсилають клієнтам повідомлень із проханням уточнити дані платіжної картки [ПІН-код, номер, строк дії та тризначний номер на звороті картки (CVV2-код)], а також логін або пароль від банківського додатку, смс-паролі, кодове слово тощо.
- **Не зазначайте фінансовий номер телефону (це номер, прив'язаний до банківських рахунків) на ресурсах з відкритим доступом.** Для торговельних майданчиків та соціальних мереж краще використовувати інший номер.
- **Установіть заборону на віддалену заміну сім-карти** (мобільні оператори з цим допоможуть).
- **Установіть блокування екрану** на Ваш смартфон (пароль, відбиток пальця тощо).
- **Не діліться паролями й реквізитами** платіжної карти ні з ким.
- У жодному разі **не пишіть ПІН-коди** на платіжній картці та паролі на аркуші паперу.

П’ять порад від українського актора театру та кіно Олексія Вертинського

Додатковий рівень захисту важливий навіть за наявності надійних паролів

Тепер у Вас є надійний пароль – замок, що оберігає скарби Вашої цифрової фортеці. Але навіть найміцніший замок потребує такого додаткового захисту, як двофакторна автентифікація. Це коли, відчинивши перший замок, Вас питають: "А чи Ви справді той, за кого себе видаєте?" І лише отримавши від Вас підтвердження, відчиняє наступний замок. Навіть якщо хтось підбере ключ до першого замка, він не зможе проникнути далі, без підтвердження.

Не здавайте в оренду свою платіжну картку

Якщо Ви даєте свою картку сторонній особі в користування (оренду), то її можуть використати, щоб приховати вкрадені гроші. Наприклад, сьогодні шахраї викрали кошти у Вашого сусіда, а завтра перераховують ці гроші з використанням картки, яку Ви здали в оренду. Так вони заплутують сліди, щоб уникнути кримінальної відповідальності.
Уявіть собі: Ви стоїте на сцені, очі глядачів спрямовані на Вас. Раптом хтось вигукує: "Здайте в оренду свої ролі! Здайте свої аплодисменти!" Це ж абсурд, чи не так? А тепер уявіть, що хтось пропонує Вам здати в оренду Вашу репутацію, Ваше ім’я, Ваш гаманець. Це не менш безглуздо!

Шахраї можуть просити в борг від імені Ваших близьких

У наші дні, як у старому голівудському фільмі, зловмисники вміло маскуються

під наших близьких. Ви навіть можете отримати послання, ніби з глибин минулого. Давній друг, з яким Ви не спілкувалися вже століття, просить у Вас невеликої позики.
Як же відрізнити справжнього друга від аферіста? Дуже просто. Зателефонуйте йому та запитайте про щось таке, що знаєте тільки Ви двоє.

Уникайте шахрайських сайтів

Шахрайські сайти – це пастки, наповнені красивими обіцянками, яскравими картинками та дешевими цінами. Вони можуть розігрувати коштовні призи, оголошувати Вас переможцями лотерей, в яких Ви не брали участі, або пропонувати легкий заробіток за розсилання інформації друзям. Вони обіцяють Вам золоті гори, але насправді хочуть лише одного – Ваших грошей.
Тож будьте обережні та перевіряйте, чи є сайт захищений, почитайте відгуки, порадьтеся з близькими, перш ніж переходити за посиланням чи зазначати свої дані на сумнівних інтернет-ресурсах.

Не передавайте свою платіжну картку чи банківський рахунок стороннім особам!

Не ставайте співучасником злочину!

Зловмисники розміщують оголошення в інтернеті, де пропонують за винагороду (приблизно 1000 гривень на добу) взяти в оренду платіжні картки та банківські рахунки.
Також можуть траплятися оголошення з пропозицією легкої роботи, де "роботодавець" просить відкрити банківський рахунок на своє ім'я для отримання та переказу коштів від імені іншої особи.
Людей, які погоджуються за винагороду надати доступ до своїх платіжних карток та банківських рахунків, називають "дропами" або "грошовими мулами".

Що це за пропозиції? І чому небезпечно на них погоджуватися?

Зловмисники використовують чужі платіжні картки та банківські рахунки як транзитні, щоб приховати кошти, які вони отримали злочинним шляхом: через торгівлю наркотиками, людьми, тероризм, шахрайство в інтернеті та інші тяжкі злочини.
Незаконні гроші рухаються з рахунку на рахунок, водночас самі злочинці залишаються в тіні. Така схема дає змогу злочинним угрупуванням "заплутати сліди" та ускладнити роботу правоохоронних органів.

Відповідальність "грошових мулів"

За такі дії може бути штраф, конфіскація майна і навіть позбавлення волі.
Зокрема, "грошові мули" несуть кримінальну відповідальність за співучасть у злочині за статтею 209 Кримінального кодексу України, що передбачає позбавлення волі на строк від 3 до 12 років.

Власник платіжної картки та банківського рахунку в такій схемі стає співучасником злочину, навіть якщо він цього не усвідомлює.

Як не стати "грошовим мулом"?

1. **Не передавайте** платіжну картку, її реквізити, реквізити рахунку в користування іншим особам!
2. **Ігноруйте** вакансії чи роботу, які передбачають продаж або оренду Вашого банківського рахунку та картки, переказ грошей між рахунками, зняття готівки для сторонніх осіб тощо.

Отримали пропозицію стати "грошовим мулом" – повідомте про це Кіберполіцію.

Стати "грошовим мулом" можна неусвідомлено, тож якщо Ви на якомусь етапі зрозуміли, що встигли погодитися на схожу пропозицію і надали дані своєї картки шахраям, слід звернутися до Кіберполіції,

залишивши заяву на сайті **ticket.cyberpolice.gov.ua**

або зателефонувавши за номером **0 800 505 170**.

Що робити, якщо у Вас виникли проблеми з погашенням кредиту?

Якщо під час обслуговування кредиту у Вас виникли проблеми з його погашенням з причин, що не залежать від Вас, Ви можете звернутися до банку чи іншої фінансової установи з проханням про реструктуризацію.

Реструктуризація – це зміна умов кредитного договору за домовленістю між банком і позичальником для надання позичальнику можливості сплачувати за кредитом з урахуванням поточного фінансового стану позичальника.

Які можуть бути варіанти реструктуризації?

- Продовження строку користування кредитом і зменшення щомісячного платежу.
- Скасування пені та штрафних санкцій.
- Списання частини боргу.

Також в окремих випадках банк / фінансова установа може запропонувати інші умови реструктуризації.

Як оформити реструктуризацію?

Потрібно звернутися до банку / фінансової установи з офіційною заявою про реструктуризацію.
Також банк / фінансова установа може запросити у Вас документи, що підтверджують виникнення обставин, за яких Ви не маєте змоги платити за кредитом. Наприклад, це може бути медична довідка про захворювання тощо.

Реструктуризація оформлюється підписанням договору, де зазначені нові умови кредиту.

Майте на увазі, що банк / фінансова установа може відмовити в реструктуризації боргу, адже реструктуризація – це право установи, а не зобов'язання.

Поділіться своєю думкою про газету та запропонуйте теми для наступних випусків!

Пройдіть опитування за QR-кодом

Головний редактор
Тетяна Машлаковська

Адреса редакції:
вул. Інститутська, 9, м. Київ, 01601
e-mail: harazd@bank.gov.ua

Інформаційний бюлетень
«Газета "Фінансова мудрість"»

Загальний тираж 448 000 шт.
Наступний номер вийде у I кварталі 2025 року