Національний банк України

Поради з кібербезпеки та схеми шахрайства у воєнний час

Сьогодні поговоримо про…

Поради з кібербезпеки у воєнний час:

- як захистити кошти на платіжні картці;
- як захистити акаунти та пристрої: смартфони та комп’ютери.

Актуальні схеми шахрайства у воєнний час:

- злам сторінки в соціальних мережах;
- шахрайство з використанням технології спуфінг;
- шахрайство під виглядом соціальних виплат;
- смс-розсилки від шахраїв.

Безпечні онлайн-покупки

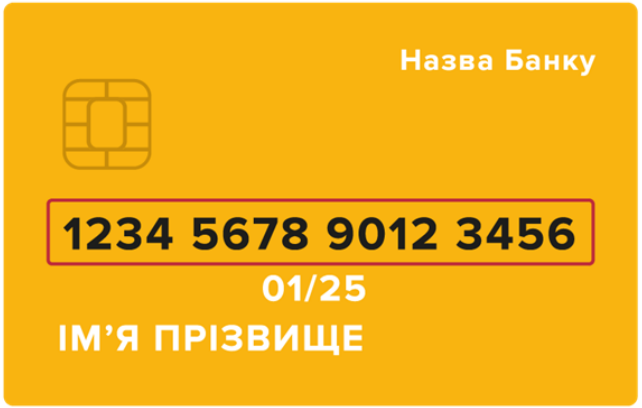
Телефонне шахрайство

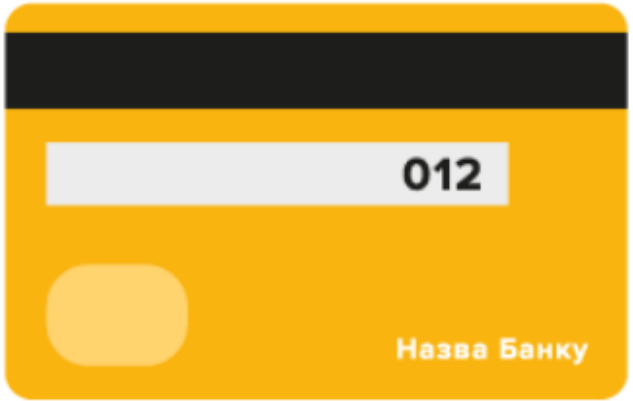
Фінансовий номер телефону

Платіжна безпека

Повідомляти можна тільки 16-значний номер картки

НІКОМУ НЕ КАЖІТЬ трьохзначний номер на звороті картки





Платіжна безпека

НІКОМУ НЕ КАЖІТЬ

- Смс-коди від банків та мобільних операторів
- Паролі до інтернет-банкінгу, акаунтів в соціальних мережах, електронної пошти

Платіжна безпека

ПІДКЛЮЧІТЬ смс-інформування стосовно операцій з платіжною карткою

Платіжна безпека

ВСТАНОВІТЬ ІНДИВІДУАЛЬНІ ЛІМІТИ
на операції з платіжною карткою

Платіжна безпека

Правильно прикривайте пін-код

Прикривайте клавіатуру під час уведення пін-коду

Платіжна безпека

Змінюйте пін-код до картки

- 1 раз на 3 місяці
- Якщо виникла підозра, що хтось його може знати

Розрахунки сматфонами

NFC (Near Field Communication) – це технологія, яка дозволяє швидко та бездротово передавати дані між пристроями на невеликій відстані.

Розраховуйтеся у торговельній мережі за допомогою смартфону з Google Pay або Apple Pay.

NFC у смартфонах чи безпечно користуватися?

Сплачувати смартфоном безпечно

Передача даних між смартфоном та терміналом здійснюються на малій відстані – в радіусі 10 см.

Смартфон не передає жодних даних про платіжну картку. Під час оплати смартфон передає одноразовий ключ, створений спеціально для кожного платежу.

ВАЖИВО! У разі фізичної втрати смартфона можуть бути певні ризики, але тільки якщо на смартфон не було встановлено жодного захисту, і його без проблем може розблокувати будь-яка особа. Адже під час оплати смартфоном, смартфон має бути розблокований.

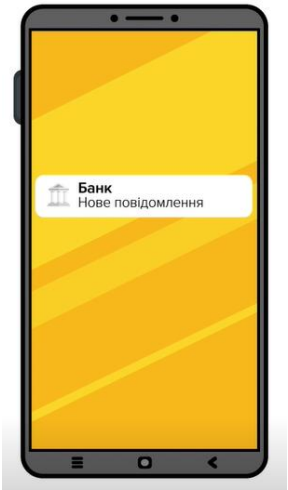
Як захистити смартфон?

Захисти свій смартфон

1. Встановіть пароль на вхід

2. Налаштуйте показ сповіщень на заблокованому екрані у такий спосіб, щоб ховати їх конфіденційний вміст

У разі втрати або крадіжки смартфона, потрібно зателефонувати до мобільного оператора та банку, щоб заблокувати свої рахунки.



Захист акаунтів

Способи захисту акаунтів в соціальних мережах:

- складний та унікальний пароль
- багатофакторна автентифікація

Захист акаунтів

Окрім шахраїв, на акаунти українців полюють російські орки

Мета - це доступ до державних реєстрів та всієї інформаційної інфраструктури країни

Обов’язок кожного у воєнний час захистити свої акаунти

Паролі

СТВОРІТЬ СКЛАДНИЙ ПАРОЛЬ
до електронної пошти, соціальних мереж та інтернет-банкінгу

Складний пароль може містити:

- 8 і більше символів
- великі та малі літери
- цифри та спеціальні знаки/символи

Пам’ятайте! Пароль має бути унікальним для кожного інтернет-банкінгу, електронної пошти, соціальної мережі тощо

Паролі

Не використовуйте для створення паролей

- Дату свого народження
- Загальновідомі комбінації: Qwerty12, Password123456, Admin1234 та подібні
- Послідовне/зворотнє написання символів або цифр

Паролі

Для створення паролю **не використовуйте** імена домашній улюбленців, свої уподобання, дату народження тощо

Murchyk134 – це слабкий пароль!

Паролі

Для створення паролей використовуйте мотиваційні фрази, рядки українських пісень, віршів, українських прислів'їв

Ой у лузі червона калина…

Багатофакторна авентифікація

Налаштовуйте багатофакторну автентифікацію всюди, де це можливо

Багатофакторна автентифікація – це коли для входу до акаунту, крім логіна та пароля, потрібно ввести код підтвердження, що приходить на смартфон, електронну скриньку або відповідний додаток

Правила кібербезпеки у воєнний час

- Перевіряйте інформацію
- Отримуйте інформацію з офіційних джерел
- Не переходьте за посиланнями від незнайомців

Чи можуть ховатися у QR-кодах шахрайські посилання?

Правила, яких потрібно дотримуватися, при скануванні QR-кодів

- скануйте QR-коди тільки із перевірених джерел, утримуйтесь від зчитування QR-кодів, які випадково потрапили вам на очі;
- якщо QR-код веде на вебсайт, упевніться у правильності написання його адреси;
- користуйтеся антивірусами, які попередять про небезпеку в разі відкриття файлів із вірусами;
- будьте особливо обачними, використовуючи QR-код для платежів;
- звертайте увагу, чи не наклеєний один QR-код поверх іншого.

Злам сторінки в соціальних мережах

Шахраї зламують сторінки в соціальних мережах та пишуть підписникам власника сторінки:

"*Привіт! Позич, будь ласка, гроші до завтра! Дуже треба!*"

ЗАПИТАЙТЕ У ДРУГА ТЕ, ЩО МОЖЕТЕ ЗНАТИ ТІЛЬКИ ВИ І ВІН

Злам сторінки в соціальних мережах

Шахраї зламують сторінки в соціальних мережах та роблять публікацію на сторінці її власника та від його імені просять фінансової допомоги на покупку амуніції у зв’язку з відбуттям на фронт

ЗАПИТАЙТЕ У ДРУГА ТЕ, ЩО МОЖЕТЕ ЗНАТИ ТІЛЬКИ ВИ І ВІН

Спуфінг

Спуфінг – це технологія, коли шахраї маскуються під офіційне надійне джерело (наприклад, банк, державну установу тощо) для отримання доступу до конфіденційних даних, що дає змогу потім викрасти кошти.

Спуфінг може бути реалізований через електронні повідомлення, смс-повідомлення, телефонні дзвінки тощо

Шахрайство під виглядом соціальних виплат

Шахраї привласнюють гроші під виглядом надання виплат українцям, які постраждали від війни. Для цього роблять смс-розсилки та розсилки в месенджерах про нарахування соціальних виплат.

Як не потрапити на гачок шахрая?

- **отримуйте інформацію лише з офіційних джерел.** Якщо оформлювали допомогу – очікуйте сповіщення про нарахування в застосунку вашого банку;
- **не переходьте за сумнівними гіперпосиланнями;**
- **тримайте в секреті:**

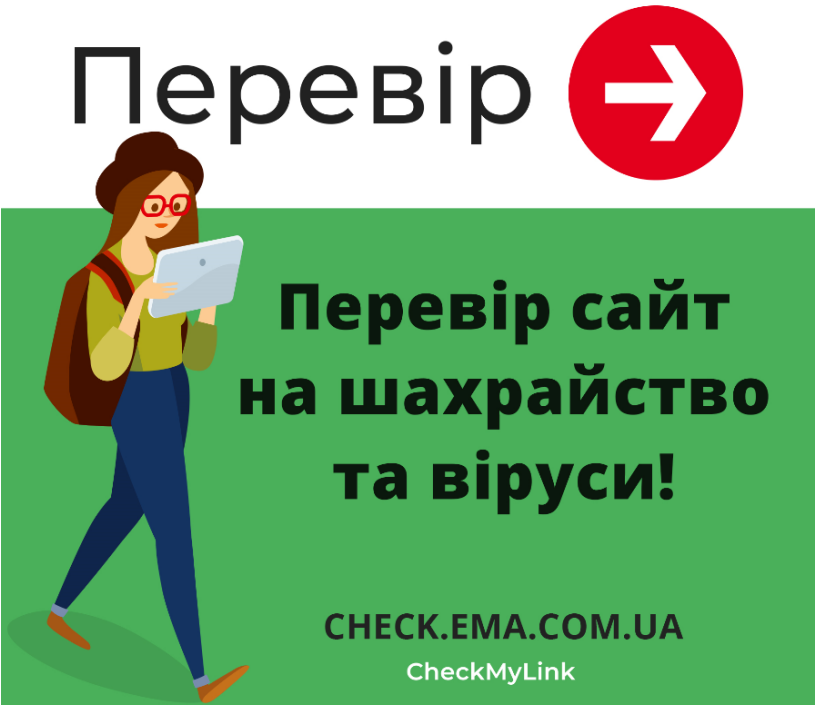
✓ тризначний номер на звороті картки;

✓ логін та пароль до інтернет-банкінгу;

✓ коди банків та мобільних операторів.

- **не вводьте реквізитів платіжних карток на незнайомих та підозрілих вебсайтах.**

Перевіряйте сайти на шахрайство



Рекомендується додатково перевірити безкоштовно сайт на шахрайство на:

- сайті Кіберполіції у розділі "STOP FRAUD"
- сервісі Асоціації "ЄМА" CheckMyLink

ВАЖЛИВО! Схема шахрайства може бути абсолютно новою або добре прихованою. Тому, крім перевірки сайту на сайті Кіберполіції у розділі "STOP FRAUD" та сервісі CheckMyLink, проводьте також власну перевірку.

Смс від шахраїв

Смс-повідомлення про надходження платежу

Шахраї розсилають смс-повідомлення клієнтам банків про нібито надходження платежу на рахунок. Такі смс-повідомлення містять фішингові посилання.

Продаж неіснуючих товарів в інтернеті

Шахраї під маскою продавців розміщують оголошення на платформі онлайн-оголошень

Псевдопродавець замість обговорення деталей угоди в особистому кабінеті торговельного майданчика, пропонує перейти в месенджер, потім надсилає посилання для оплати, яке веде на фішинговий сайт.

Ознаки псевдопровдаця

- Занижена вартість товару
- Виманює секретні реквізити картки
- Переводить спілкування з особистого кабінету на сайті оголошень в месенджер
- Просить зняти ліміт з картки для проведення оплати.

Шахраї створюють ілюзію роботи справжнього магазину:

- швидко відповідають на повідомлення
- допомагають підібрати розмір
- консультують з приводу характеристик товару
- обіцяють швидку доставку.

Правила безпечних онлайн-покупок

- **не переходьте в месенджери,** коли купуєте на торговому онлайн-майданчику/дошці оголошень;
- **надавайте перевагу післяплаті;** Остерігайтеся рекламних оголошень, які заманюють купити якісні речі за мінімальними цінами.
- **не переходьте за посиланнями від незнайомців;**
- **не вводьте реквізитів платіжних карток на незнайомих та підозрілих вебсайтах.**

Телефонне шахрайство

Телефонне шахрайство – це вид шахрайства, коли шахрай телефонує і переконує жертву повідомити особисту, фінансову чи конфіденційну інформацію або переказати гроші.

На яку інформацію полює шахрай?

- Реквізити картки
- Паролі
- Смс-коди від банків та мобільних операторів

Ознаки телефонної розмови із шахраєм

- Тривожна ситуація
- Психологічний тиск
- Поспіх
- Несподіваний виграш. Гроші як приманка

Телефонне шахрайство

Телефонні дзвінки від імені працівників банків

Під час таких телефонних розмов шахрай може:

- **варіант 1** – запевняти, що до рахунків громадянина отримали доступ сторонні;
- **варіант 2** – просити громадянина надати інформацію про картки та рахунки через планову перевірку даних у зв’язку з війною;
- **варіант 3** – повідомляти про кібератаку на ІТ-систему банку;
- **варіант 4** – просити встановити програму віддаленого доступу для посилення заходів безпеки.

Що робити, якщо на дроті шахрай?

КЛАДІТЬ СЛУХАВКУ

Телефонуйте на номер, що вказаний на звороті платіжної картки

Випадково повідомили реквізити картки та пароль шахраю?

НЕГАЙНО ЗАБЛОКУЙТЕ КАРТКУ

Фінансовий номер телефону

Фінансовий номер телефону – це номер, який прив’язаний до банківських рахунків.

На цей номер надходять:

- коди підтвердження операцій
- паролі від банків
- інформація про баланс коштів на рахунках

Схема крадіжки фінансового номеру телефону

Сценарій шахрайства

Шахрай телефонує від імені працівника мобільного оператора та пропонує перейти на нові поліпшені стандарти зв’язку. Для підтвердження просить назвати код із смс-повідомлення.

Відключіть послугу віддаленої заміни сім-картки у свого мобільного оператора.

Як захистити свій фінансовий номер телефону?

Зареєструйтеся в онлайн-кабінеті мобільного оператора

Зареєструйте сім-картку на свій паспорт

Тримайте в секреті

- Логін та пароль до онлайн-кабінету мобільного оператора
- Смс-коди мобільного оператора

Прокачайте свої знання з платіжної безпеки

Сайт НБУ з платіжної безпеки

#ШахрайГудбай