Національний банк України

Поради з кібербезпеки та схеми шахрайства у воєнний час

Урок з фінансової грамотності в старшій школі

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;
- фейковий збір коштів на допомогу;
- фейкові смс-розсилання.

Безпечні онлайн-покупки

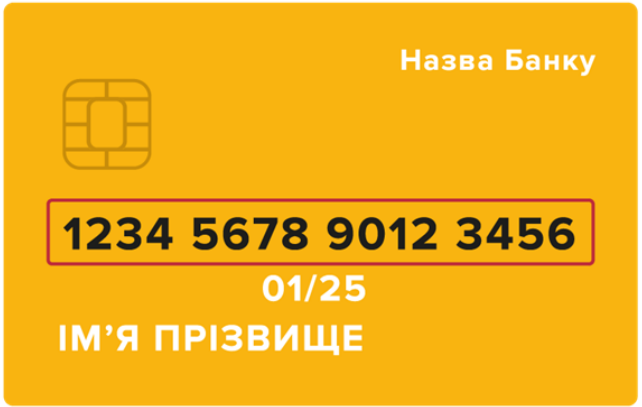
Телефонне шахрайство

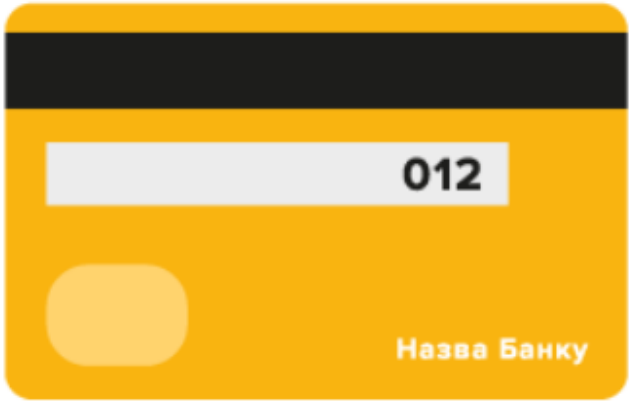
Фінансовий номер телефону

Платіжна безпека

Повідомляти можна тільки 16-значний номер картки

НІКОМУ НЕ КАЖІТЬ тризначний 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 із платіжною карткою

Платіжна безпека

УСТАНОВІТЬ ІНДИВІДУАЛЬНІ ЛІМІТИ
на операції з платіжною карткою

Платіжна безпека

Правильно прикривайте клавіатуру банкомата чи платіжного термінала 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.

Додатковий захист для карток та рахунків

Додаткові види захисту для карток та рахунків:

- розраховуйтеся в торговельній мережі за допомогою смартфона з Google Pay або Apple Pay. Тоді ніхто не побачить реквізити картки;
- використовуйте голосову біометрію.

Захист акаунтів

Способи захисту акаунтів у соціальних мережах:

- складний та унікальний пароль;
- багатофакторна автентифікація;
- сервіси VPN.

Захист акаунтів

Крім шахраїв, на акаунти українців полюють російські хакери.

Мета – 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 паролів:

- дату свого народження;
- загальновідомі комбінації: Qwerty12, Password123456, Admin1234 та подібні;
- послідовне/зворотнє написання символів або цифр.

Паролі

Для створення пароля **не використовуйте** імена домашніх улюбленців, свої уподобання, дату народження тощо.

Murchyk134 – це слабкий пароль!

Паролі

Для створення паролів 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 акаунта, крім логіна та пароля, потрібно ввести код підтвердження, що приходить на смартфон, електронну скриньку або відповідний застосунок.

Що таке VPN?

VPN – це віртуальна приватна мережа.

VPN використовують для захисту даних та власної безпеки.

VPN — це якісний спосіб захистити спілкування в соціальних мережах.

Для чого використовують VPN?

- VPN запобігає отриманню хакерами доступу до важливої інформації, яку людина вводить на вебсайтах, наприклад, до логінів та паролів, даних платіжних карток тощо;
- VPN забезпечує захист під час підключення до загальнодоступних Wi-Fi-мереж;
- VPN запобігає завантаженню шкідливих програм на пристрій;
- приховує місцезнаходження.

Як обрати, який VPN-сервіс установити?

Безкоштовні VPN-сервіси, які радить Кіберполіція:

- **Windscribe;**
- **Hide.me;**
- **Press-vpn;**
- **Hotspot Shield.**

VPN-сервіси

Недоліки VPN:

- підключення до VPN **не завжди є безпечним**, як може здаватися. Підключаючись до мережі "Інтернет" через VPN, ми отримуємо доступ до інтернету через сервер компанії – постачальника VPN. Можливо, наші технічні дані десь зберігаються і до них мають доступ треті особи;
- підключення до VPN може **значно вплинути на швидкість** з'єднання з мережею "Інтернет";
- безкоштовні VPN мають такі **недоліки:** дратівлива реклама, обмежений обсяг даних, повільне з'єднання, нестабільність роботи тощо.

Правила кібербезпеки у воєнний час:

- перевіряйте інформацію;
- отримуйте інформацію з офіційних джерел;
- не переходьте за посиланнями від незнайомців.

Злам сторінки в соціальних мережах

Шахраї зламують сторінки в соціальних мережах і роблять публікацію на сторінці її власника, 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

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

Фейковий збір коштів на допомогу

Шахраї роблять фейкові оголошення зі збору грошей.

Є випадки, коли шахраї знаходять фото потерпілих людей у інтернеті й використовують їх у своїх оголошеннях.

Фейковий збір коштів на допомогу

Шахраї створюють фішингові (шахрайські) сайти, які схожі на сайти справжніх благодійних фондів, де нібито можна переказати кошти на підтримку Збройних сил України.

Як не потрапити на гачок шахрая?

- Перевіряйте правильність назви сайтів, на які переходите та вводите свої персональні дані.
- Якщо отримали посилання на сайт благодійного фонду в месенджері, смс чи e-mail або побачили відповідне посилання в публікації в соціальних мережах не від офіційного джерела, не переходьте за посиланням. Краще **введіть у пошуковій системі назву необхідного сайту і лише тоді переходьте на вебресурс.**

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

Видаючи себе продавцями, шахраї "продають" товари, на які зараз є великий попит та яких не вистачає на полицях магазинів.

Які можуть бути варіанти реалізації цієї схеми?

Шахраї можуть створювати фейкові інтернет-магазини або розміщувати оголошення на онлайн-майданчику оголошень.

Ознаки псевдопродавця:

- занижена вартість товару;
- поспішає з оплатою;
- не знає характеристик товару;
- виманює секретні реквізити картки;
- переводить спілкування з особистого кабінету на сайті оголошень в месенджер;
- просить зняти ліміт із картки для проведення оплати.

Правила безпечних онлайн-покупок

- Для розрахунків у інтернеті створіть окрему віртуальну картку.
- Сайти, які приймають онлайн-платежі мають бути захищеними, для цього в назві адреси вони мають містити **https://** та значок "  ". На сайті мають бути значки захисту онлайн-покупок від платіжних систем **Verified by Visa та MasterCard SecureCode.**

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?

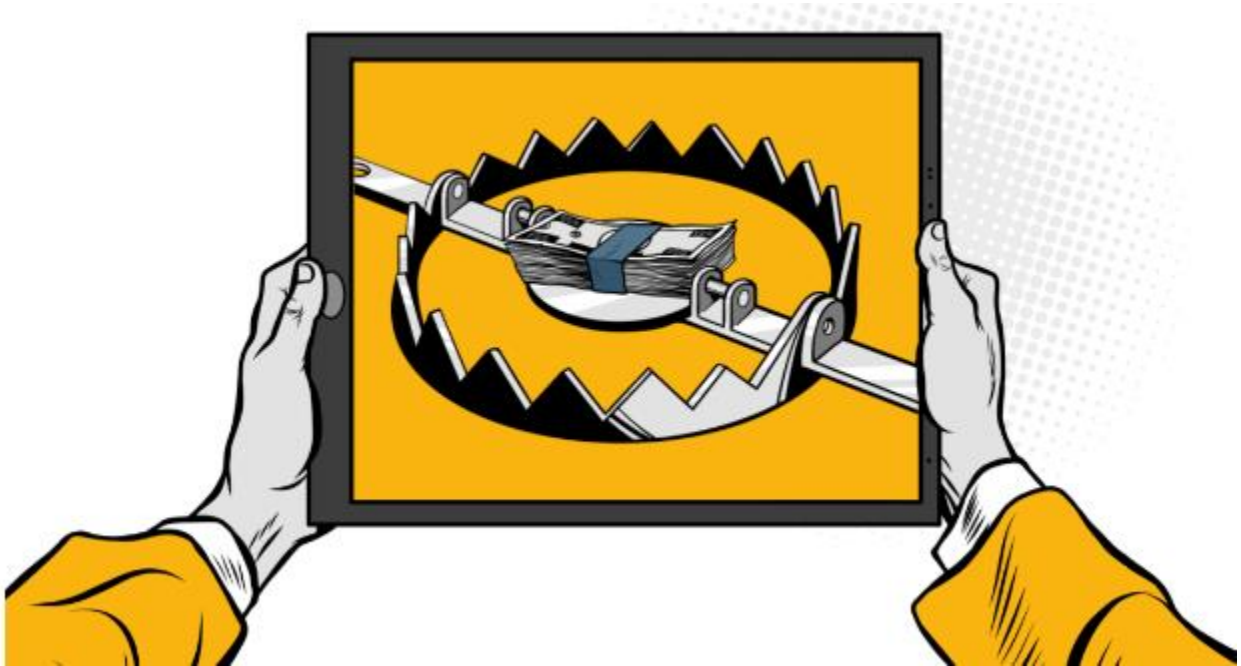
- Реквізити картки.
- Паролі.
- Смс-коди від банків та мобільних операторів.

Ознаки телефонної розмови із шахраєм

- Тривожна ситуація.
- Психологічний тиск.
- Поспіх.

Ознаки телефонної розмови з шахраєм

Несподіваний виграш. Гроші як приманка.



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 номера телефону

Сценарій шахрайства

Шахрай телефонує та мовчить, а потім поповнює рахунок.

Отримує історію дзвінків та відновлює сім-картку, як втрачену.

ЗАРЕЄСТРУЙТЕ СІМ-КАРТКУ НА СВІЙ ПАСПОРТ

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

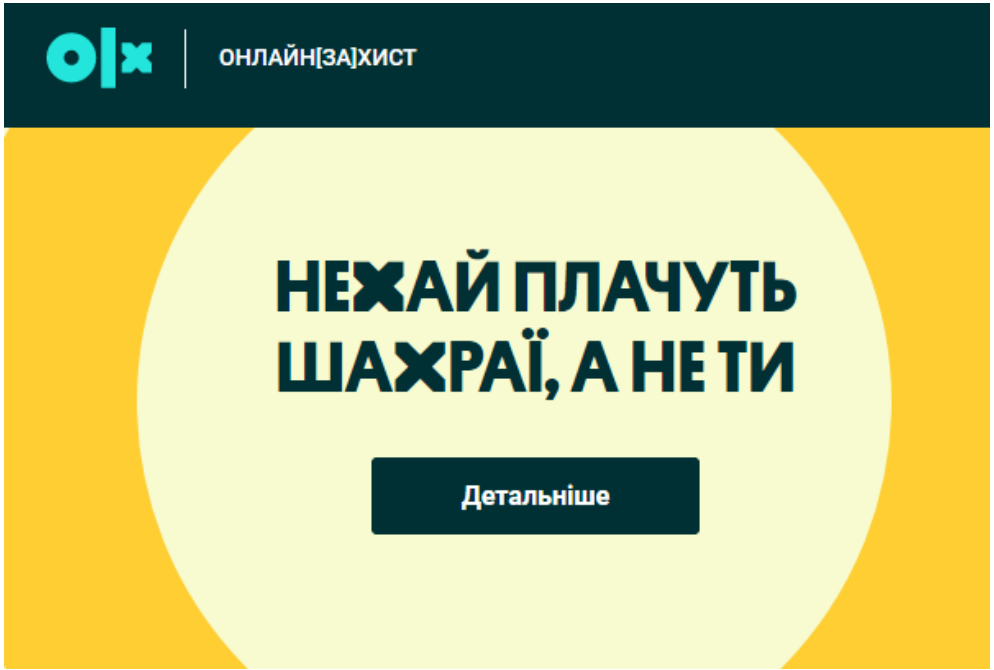
Онлайн-гра "Здолай шахрая"

Прокачайте свої знання з платіжної безпеки

Серіал "Школа платіжної грамотності"

Прокачайте свої знання з платіжної безпеки

Сайт про безпечний онлайн-шопінг



Прокачайте свої знання з платіжної безпеки

Сайт НБУ з платіжної безпеки

#ШахрайГудбай