Національний банк України

ПЛАН-КОНСПЕКТ
уроку з фінансової грамотності "Поради з кібербезпеки та схеми шахрайства у воєнний час"

для учнів старшої школи

ЗМІСТ

Тема уроку: "Поради з кібербезпеки та схеми шахрайства у воєнний час"

Мета уроку: познайомити учнів із правилами платіжної безпеки, вберегти учнів від випадків шахрайства, поліпшити обізнаність учнів про кібергігієну та сформувати культуру безпечної поведінки у віртуальному просторі.

Терміни, про які учні дізнаються під час уроку: фінансовий номер телефону, багатофакторна автентифікація.

Розгорнутий план уроку

1. **Поради з кібербезпеки у воєнний час.**
   - Як захистити кошти на платіжній картці?
   - Як захистити акаунти та пристрої: смартфони та комп'ютери?

2. **Актуальні схеми шахрайства у воєнний час.**
   - Злам сторінки в соціальних мережах.
   - Фейковий збір коштів на допомогу.
   - Фейкові смс-розсилання.

3. **Правила безпечних онлайн-покупок.**
   - Продаж неіснуючих товарів у інтернеті.
   - Ознаки псевдопродавця.
   - Як не потрапити на гачок шахрая?

4. **Телефонне шахрайство.**
   - Що таке телефонне шахрайство?
   - Ознаки телефонної розмови з шахраєм.
   - Що робити, якщо на зв'язку шахрай?

5. **Фінансовий номер телефону.**
   - Що таке фінансовий номер телефону?
   - Схеми крадіжки фінансового номера телефону.
   - Як захистити свій фінансовий номер телефону?

6. **Ресурси для учнів для поліпшення власних навичок із платіжної безпеки.**
   - Онлайн-гра "Здолай шахрая".
   - Серіал "Школа платіжної грамотності".
   - Сайт про безпечний онлайн-шопінг.
   - Сайт НБУ з платіжної безпеки #ШахрайГудбай.

Після завершення уроку школярі знатимуть:
- основні правила платіжної безпеки;
- як захистити свої акаунти та пристрої;
- що таке фінансовий номер телефону та навіщо він потрібен;
- актуальні схеми шахрайства у воєнний час та як від них вберегтися;

- правила онлайн-покупок.

Після завершення уроку учні будуть вміти:

- створювати надійні паролі;
- встановлювати багатофакторну автентифікацію;
- розпізнавати шахраїв під час телефонних розмов та в інтернет-мережі;
- здійснювати онлайн-покупки з дотриманням правил платіжної безпеки.

Матеріали є доповненням до проведення уроків з предметів "Фінансова грамотність" або можуть використовуватися для проведення класної години.

Конспект уроку

Питання 1. Поради з кібербезпеки у воєнний час.

Лектор демонструє слайди 1-2

Привітання, знайомство та інформування про тему заняття.

Доброго дня, дорогі учні.

Розпочнімо наше заняття із запитання: чи є у вас платіжні картки та як часто ви ними користуєтесь?

(відповіді дітей).

Дякую за відповіді. Карткою потрібно не лише вміти користуватися, а й знати, яку інформацію можна повідомляти стороннім особам, а яку – ні, щоб вберегти свої кошти від шахраїв. Адже в світі понад половина карткових шахрайств відносяться до соціальної інженерії, коли люди самі переказують гроші шахраям або розкривають дані своїх карток.

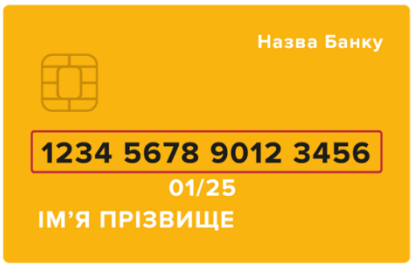
Питання для аудиторії: А чи знаєте ви, яку інформацію про платіжну картку можна повідомляти стороннім особам?

(відповіді дітей).

Друзі, дякую вам за відповіді.

Сьогодні на занятті ми з вами поліпшимо свої знання з кібербезпеки та поговоримо про:

- кібербезпеку у воєнний час;
- актуальні схеми шахрайства у воєнний час;
- безпечні онлайн-покупки;
- телефонне шахрайство;
- фінансовий номер телефону.

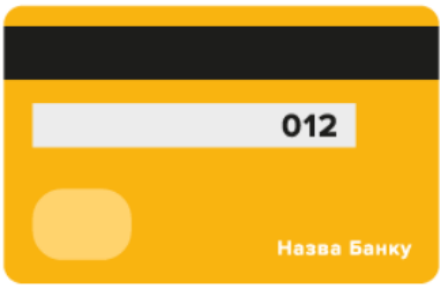


Лектор демонструє слайд 3

Отже, спершу поговоримо про платіжну безпеку.

Не можна розголошувати всі реквізити платіжної картки.

16-значний номер картки – єдине, що ви можете повідомити. Цю інформацію повідомляти безпечно, її достатньо для того, щоб на вашу картку перерахували гроші.



Тримайте в секреті три цифри на звороті картки та термін дії картки.

Якщо телефоном просять повідомити три цифри на звороті картки – це перша ознака шахрайства.

Лектор демонструє слайд 4

Також необхідно тримати в секреті:

- смс-коди від банків та мобільних операторів;
- паролі до інтернет-банкінгу, акаунтів у соціальних мережах, електронної пошти.

Цю інформацію за жодних умов не будуть у вас запитувати телефоном працівники банків, мобільних операторів та будь-яких державних установ. Якщо про таке питають, – це 100% шахраї.

Лектор демонструє слайд 5 та 6

Контролюйте рух коштів на рахунку.

Підключіть послугу інформування про операції з платіжною карткою та встановіть індивідуальні ліміти на операції з платіжною карткою.

Таку послугу можна підключити у відділенні під час оформлення картки, зателефонувати до контакт-центру вашого банку або за допомогою онлайн-банкінгу.

Лектор демонструє слайд 7

Прикривайте клавіатуру рукою під час введення пін-коду.

Так, потрібно прикривати пін-код не від людей, які стоять позаду в черзі до банкомата, а від мікрокамери, яку шахраї могли встановити біля банкомата.

Скімінг – це вид шахрайства, коли шахраї роблять копію вашої платіжної картки за допомогою спеціального шахрайського пристрою, який вони встановлюють у кардрідер. Але така скопійована картка – ніщо без пін-коду. Щоб дізнатися пін-код, шахраї використовують приховану мікрокамеру.

Мікрокамера може бути встановлена прямо над головою або біля самої клавіатури. Шукати її не потрібно, але необхідно прикривати клавіатуру під час введення пін-коду так, як показано на слайді.

Лектор демонструє слайд 8

Змінюйте пін-код до картки:

- 1 раз на 3 місяці;
- якщо виникла підозра, що хтось, крім вас, може його знати.

Лектор демонструє слайд 9

Також можна використовувати додатковий захист для карток та рахунків.

Щоб убезпечити реквізити вашої картки від сторонніх очей, можна розраховуватися смартфоном. Здійснюйте оплату в магазинах за допомогою смартфона з Google Pay або Apple Pay – тоді ніхто не побачить реквізити картки.

Чому це безпечно?

Наприклад, для здійснення оплати з Apple Pay необхідне підтвердження Face ID, Touch ID або пароля.

Touch ID – це спосіб автентифікації через відбиток пальця.

Face ID — це спосіб автентифікації через розпізнавання обличчя.

В обох випадках дані картки надійно зашифровані, номер картки перетворюється на унікальний платіжний код, який неможливо підробити.

Використовуйте голосову біометрію.

Наприклад, клієнти ПриватБанку можуть скористатися технологією захисту карток та рахунків, яка називається “Голосова біометрія”.

Голосова біометрія – це технологія для створення біометричних голосових зліпків клієнтів, що дає змогу ідентифікувати особу за сукупністю унікальних характеристик голосу та забезпечує додатковий захист рахунків і особистих даних.

Тобто, якщо ви зателефонуєте до контакт-центру банку, система швидко вас розпізнає за голосом.

Така ідентифікація прискорює обслуговування та захищає ваші кошти, оскільки ніхто, крім вас, не зможе здійснити жодної операції, звернувшись до контакт-центру банку від вашого імені.

Лектор демонструє слайд 10

Є кілька ефективних способів захисту акаунтів у соціальних мережах:

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

Щоб ваші дані залишалися у безпеці, потрібно дотримуватися простих рекомендацій.

Лектор демонструє слайд 11

Крім шахраїв, на акаунти українців полюють російські хакери.

Згідно з інформацією від Державної служби спеціального зв’язку та захисту інформації доступ до приватних телефонів та комп’ютерів громадян України – це один із векторів атак російських хакерів. Російські хакери постійно намагаються

отримати інформацію про персональні дані звичайних громадян, доступи до їх облікових записів тощо.

Яка кінцева мета російських хакерів?

Доступ до державних реєстрів та всієї інформаційної інфраструктури країни. Зокрема, вони намагаються її досягти через приватні застосунки та звичайних користувачів.

Тому захист власних пристроїв – це не лише запобіжний захід, який вбереже ваші кошти, це передусім безпека інформаційної інфраструктури всієї країни.

Обов'язок кожного у воєнний час захистити свої акаунти.

Лектор демонструє слайд 12

Пароль – це ключ до ваших даних.

Створюйте складні паролі.

Надійні та унікальні паролі – запорука безпеки ваших коштів. Раджу ставитися до цього з повною серйозністю і відповідальністю!

Створіть складні, а головне – різні паролі 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.

Щоб створити надійний пароль, змінюйте літери на цифри і спеціальні символи за тільки вам відомою системою. Поєднуйте для створення пароля слова, які пов'язані між собою.

Паролі мають відрізнятися!

Пам'ятайте! Пароль має бути унікальним для кожного інтернет-банкінгу, облікових записів Google/ICloud, електронної пошти, соціальних мереж, ігрових акаунтів тощо.

Якщо просунутий зловмисник отримає доступ до вашого пароля з інтернет-крамниці, то перше, що він зробить, – спробує той самий пароль і до інтернет-банкінгу, до електронної пошти або до акаунта в соціальних мережах.

Злочинці користуються тим, що люди, як правило, використовують однакові або схожі паролі до розважальних і фінансових сервісів. Тому, зламавши розважальний, легко добирають пароль і до фінансового сервісу.

Лектор демонструє слайд 13

Не використовуйте для паролей:

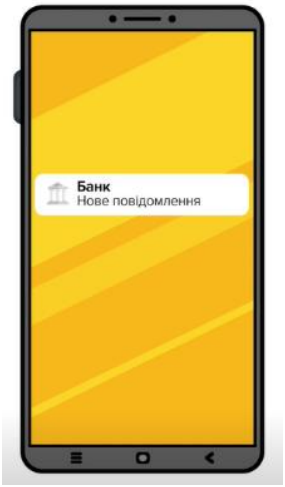
- дату свого народження;
- загальновідомі комбінації: Qwerty12, Password123456, Admin1234 та подібні;

- послідовне/зворотнє написання символів або цифр.

Подібні паролі шахраї можуть легко підібрати.

Лектор демонструє слайд 14

У паролях не можна використовувати нічого, що буде асоціюватися з вашими захопленнями, сім'єю чи тим, що (хто) людину оточує: імена близьких родичів, улюблена пісня, книга або художник, домашня тварина, улюблене місто тощо.



Щоб захистити смартфон та особисту інформацію, яку він містить, потрібно встановити пароль для входу до смартфона або використовувати біометрію (сканер відбитка пальця, розпізнавання обличчя), якщо така функція є у вашому пристрої.

Для захисту смартфона налаштуйте показ сповіщень на заблокованому екрані у такий спосіб, щоб приховати їх конфіденційний вміст.

Використовуйте лише ліцензійні програми, мобільні застосунки та систематично їх оновлюйте.

Лектор демонструє слайди 15

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

Наприклад, для створення пароля можна використати рядки української пісні "Ой у лузі червона калина". Такий пароль легко запам'ятати та приємно згадувати.

Але, звісно, краще використовувати рядки менш відомих пісень.

Такий патріотичний пароль навряд чи зможе підібрати шахрай, а російському хакеру він теж буде не по зубах.

Трансформуйте парольні фрази в паролі, змінюючи літери на цифри і спеціальні символи за тільки вам відомою системою.

Лектор демонструє слайд 16

Всюди, де це можливо, використовуйте багатофакторну автентифікацію.

Багатофакторна автентифікація – це коли для входу до акаунта, окрім логіна та пароля потрібно ввести код підтвердження, що приходить на телефон, електронну скриньку або відповідний додаток.

Лектор демонструє слайд 17

VPN — це якісний спосіб захистити ваше спілкування в соціальних мережах.

VPN – це віртуальна приватна мережа.

Для чого використовувати VPN?

Перш за все, для захисту даних та власної безпеки.

Лектор демонструє слайд 18

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;
- забезпечує захист під час підключення до загальнодоступних Wi-Fi мереж;
- запобігає завантаженню шкідливих програм на пристрій;
- приховує місцезнаходження.

Лектор демонструє слайд 19

Як обрати, який VPN-сервіс установити?

На ринку є сотні видів VPN.

Ось безкоштовні VPN-сервіси, які радить Кіберполіція:

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

Лектор демонструє слайд 20

Але у VPN є певні недоліки. Наприклад:

- підключення до VPN не завжди є таким 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;
- безкоштовні VPN мають такі недоліки, як дратівлива реклама, обмежений обсяг даних, повільне з'єднання, нестабільність роботи тощо.

Лектор демонструє слайд 21

Дотримуйтеся таких правил кібербезпеки у воєнний час:

- перевіряйте інформацію. В мережі "Інтернет" дуже багато фейків, мета яких ошукати громадян та посіяти паніку серед населення;
- отримуйте інформацію з офіційних джерел;
- не переходьте за посиланнями від незнайомців. Шахрайські посилання мають на меті зараження пристроїв вірусом або викрадення персональних даних, секретних карткових реквізитів;
- установіть антивірус, оновлюйте застосунки на своєму смартфоні та програмне забезпечення на комп’ютері.

Питання 2. Актуальні схеми шахрайства у воєнний час.

Лектор демонструє слайд 22

Розглянемо актуальні у воєнний час сценарії шахрайства.

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.

Лектор демонструє слайд 23

Можливий також і інший варіант цієї схеми: шахраї зламують сторінку людини в соціальних мережах, наприклад, "Фейсбук", "Інстаграм", розсилають усім підписникам однакові повідомлення такого змісту: "Привіт! Позич, будь ласка, гроші до завтра! Дуже треба!"

Суму шахраї зазначають різну.

Що робити, якщо отримали таке повідомлення від друга чи побачили публікацію на сторінці друга про фінансову допомогу?

Звичайно, подібна ситуація може статися з кожним. І у друга могло виникнути скрутне становище.

Перш ніж позичати гроші чи надсилати на картку фінансову допомогу:

- **Запитайте друга те, що можете знати тільки він і ви.**

Таке питання одразу викриє шахрая.

- **Перетелефонуйте другу.**

За номером, який ви точно знаєте, а не на той, що зазначений на сторінці в соціальних мережах. Якщо шахрай зламав сторінку, то міг змінити номер телефону в профілі жертви.

- **Напишіть спільним друзям у соціальних мережах, чи не отримували вони подібних повідомлень від друга.** Шахраї, як правило, одночасно роблять розсилання на всіх підписників зламаної сторінки.

Щоб такого не трапилося з вами, створюйте складні та унікальні паролі для кожного облікового запису та встановлюйте багатофакторну автентифікацію, де це можливо.

Лектор демонструє слайд 24

Розглянемо наступний сценарій шахрайства про фейковий збір коштів на допомогу.

Шахраї роблять фейкові оголошення зі збору грошей на лікування дітей, які нібито постраждали від військової агресії. Є випадки, коли шахраї знаходять фото потерпілих людей в інтернеті і збирають гроші на допомогу "постраждалим".

Лектор демонструє слайд 25

Є інший варіант цієї схеми, коли шахраї створюють фішингові (шахрайські) сайти, які схожі на сайти справжніх благодійних фондів, де нібито можна переказати кошти на підтримку Збройних сил України.

Лектор демонструє слайд 26

Як не потрапити на гачок шахрая?

Перевіряйте правильність назви сайтів, на які переходите і вводите свої персональні дані.

Якщо ви отримали посилання на сайт благодійного фонду в месенджері, смс чи на 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, а потім вже переходьте на вебресурс.

Лектор демонструє слайд 27

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

Не переходьте за посиланнями – через них шахраї можуть заволодіти вашими картковими реквізитами.

Шахрайські посилання також можуть надсилатися з метою викрадення персональних даних та зараження пристроїв вірусом.

Крім смс, аферисти можуть надіслати шкідливі посилання в месенджер та на e-mail.

Питання 3. Правила безпечних онлайн-покупок

Лектор демонструє слайд 28

В окремих регіонах, звільнених від окупантів, українці повертаються до своїх домівок, намагаючись відновити колишнє життя.

Водночас повертаються схеми шахрайства, що були найпоширенішими до війни.

Йдеться про продаж неіснуючих товарів у інтернеті.

Під маскою продавців шахраї "продають" товари, на які зараз є великий попит та яких не вистачає на полицях магазинів.

Зокрема, серед таких товарів трапляється корм для тварин.

Які можуть бути варіанти реалізації цієї схеми?

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

Аферисти переконують здійснити передплату за товар, а потім зникають.

Також шахраї можуть надсилати фішингові посилання для сплати.

Після того, як людина переходить за фішинговим посиланням та здійснює оплату, шахраї дізнаються секретні банківські реквізити та привласнюють гроші на рахунках покупців. Схеми не нові, але, на жаль, дієві.

Лектор демонструє слайд 29

Як розпізнати псевдопродавця?

Ознаки псевдопродавця:

- продає товар із заниженою вартістю;
- поспішає з оплатою;
- не знає характеристик товару;
- виманює секретні реквізити картки;
- переводить спілкування з особистого кабінету на сайті оголошень у месенджер;
- просить зняти ліміт із картки для проведення оплати.

Лектор демонструє слайд 30

Щоб купувати онлайн безпечно, потрібно дотримуватися простих правил:

- звертати увагу на те, що сайти, які приймають онлайн-платежі, мають бути захищеними, тобто в назві адреси вони мають містити: https:// та значок " ";
- пильнувати, щоб на сайті продавця були значки захисту онлайн-покупок від платіжних систем – Verified by Visa та MasterCard SecureCode;
- купувати та сплачувати лише на перевірених сайтах, надавати перевагу післяоплаті;
- не переходити в месенджери, якщо купуєте на онлайн-майданчику оголошень, обговорюйте деталі угоди тільки в чаті цієї платформи;
- перевіряти правильність назви необхідного сайту. Адреси справжнього та шахрайського сайтів можуть бути майже однаковими, за винятком одного чи кількох символів;
- завжди тримати в секреті: тризначний номер на звороті картки, коди банків, паролі до інтернет-банкінгу.

Питання 4. Телефонне шахрайство.

Лектор демонструє слайд 31

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.

Лектор демонструє слайд 32

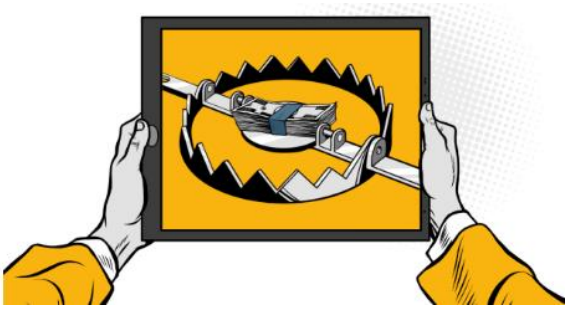
Сценаріїв телефонного шахрайства може бути безліч, але ціль у шахраїв одна – отримати секретну інформацію та вкрасти гроші з рахунків.

Ознаки телефонної розмови з шахраєм:

- тривожна ситуація;
- психологічний тиск;
- поспіх.

Лектор демонструє слайд 33

Несподіваний виграш. Гроші як приманка.



Гроші як приманку дуже часто використовують шахраї у своїх схемах, не лише у телефонному шахрайстві і в шахрайстві в інтернеті.

Як захиститися?

- Не вірити в дивовижні виграші.
- Перш ніж проходити будь-яке опитування, необхідно перевірити всю інформацію про нього: назву акції, адресу сайту, відгуки в інтернеті.
- Пам’ятати: комісії та податки сам отримувач виграшу не сплачує! Вони завжди утримуються з суми призу (виграшу).

Лектор демонструє слайд 34

Що робити, якщо на зв’язку шахрай?

Кладіть слухавку!

Випадково повідомили шахраю секретні реквізити картки та паролі?

Заблокуйте вашу картку, картковий рахунок та/або доступ до інтернет-банкінгу.

Для цього зателефонуйте на гарячу лінію банку, вказану на звороті картки.

Краще збережіть номер телефону банку в своїй телефонній книзі, щоб завжди мати його під рукою.

<u>Питання для аудиторії:</u> чи стикалися ви чи ваші батьки з телефонним шахрайством?

(відповіді дітей).

Друзі, дякую вам за відповіді.

Питання 5. Фінансовий номер телефону.

Лектор демонструє слайд 35

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.

Якщо шахрай присвоїть собі ваш фінансовий номер телефону, то зможе вкрасти гроші з рахунків, тому важливо захищати свій фінансовий номер телефону.

Лектор демонструє слайд 36

Приклад схеми крадіжки фінансового номера телефону.

Щоб вкрасти фінансовий номер, шахрай відновлює сім-картку, як "втрачену".

Що для цього потрібно?

Для відновлення сім-картки мобільні оператори часто просять історію дзвінків та інформацію про останнє поповнення мобільного рахунку.

Що робить шахрай?

- телефонує жертві з незнайомого номера,
- мотивує зателефонувати на різні номери,
- поповнює рахунок на незначну суму та відновлює сім-картку.

Також можливий інший варіант цієї схеми: жертві телефонує шахрай від імені працівника мобільного оператора, пропонує перейти на нові поліпшені стандарти зв'язку. Для підтвердження потрібно лише назвати код із смс-повідомлення.

Що ж це за код?

Насправді це пароль для входу в персональний кабінет жертви на сайті мобільного оператора.

Шахрай швиденько здійснює віддалений перевипуск сім-картки.

З цього часу сім-картка жертви не працює, а фінансовим номером телефону розпоряджається шахрай.

Шахрай має змогу отримати доступ до:

- телефонної книги та смс-повідомлень;
- акаунтів у соціальних мережах;
- Google Account, електронної пошти тощо.

Зрештою, шахрай може:

- вкрасти гроші з банківських рахунків;
- оформити онлайн-кредити;
- від імені жертви просити грошей у друзів у соціальних мережах.

Завжди тримайте в секреті смс-паролі мобільного оператора.

Лектор демонструє слайд 37

Як захистити свій фінансовий номер телефону?

Як захистити фінансовий номер?

- Пройти ідентифікацію у свого мобільного оператора та зареєструвати сім-картку на свій паспорт.
- Зареєструватися в онлайн-кабінеті мобільного оператора.
- Відключити послугу віддаленої заміни сім-картки у свого мобільного оператора.

Тримайте в секреті:

- логін та пароль до онлайн-кабінету мобільного оператора,
- смс-коди мобільного оператора,
- серійний номер сім-картки, PUK-код, кодове слово (якщо є).

Питання 5. Ресурси для учнів для поліпшення власних навичок із платіжної безпеки.

Лектор демонструє слайд 38

Щоб прокачати свої навички з платіжної безпеки, раджу вам такі ресурси:

онлайн-гра "Здолай шахрая" https://game.ema.com.ua/

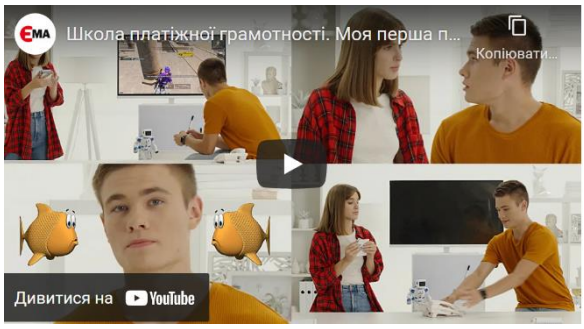
Антишахрайська онлайн-гра "Здолай шахрая", розроблена Асоціацією "ЄМА", покликана допомогти громадянам розвивати й поліпшувати власні навички з кібербезпеки та захисту від більше ніж 80 видів платіжного та інтернет-шахрайства!

У легкому та веселому форматі, максимально наближеному до реальних шахрайських ситуацій, можна дізнатися все про найактуальніші шахрайські загрози та головні правила захисту й кібербезпеки!

Навчайтеся захищати свою платіжну картку й кошти, граючи в гру. Створюйте наднадійні паролі та учіться відрізняти безпечні мобільні застосунки від потенційно шкідливих. Захищайтеся від фішингу, вішингу, скімінгу.

Лектор демонструє слайд 39

Серіал "Школа платіжної грамотності", посилання на серіал: http://surl.li/bzvrz



Серіал для старшокласників.

Рекомендуємо до перегляду серіал "Школа платіжної грамотності".

П’ять серій у форматі коротких історій від Соні та Сані.

Про що серіал?

Про сучасні платіжні технології:

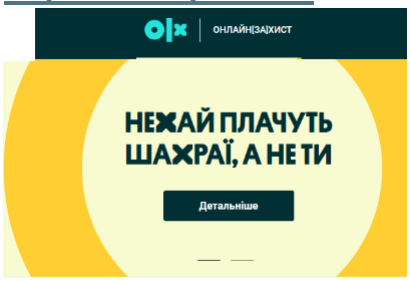
- Як самостійно та швидко оформити платіжну картку?
- Як оплатити покупки смарт-годинником чи смартфоном?
- Як безпечно розраховуватися в інтернеті?

- Як перевіряти платіжні сайти?

Тільки живі приклади без нудного пояснення.

Лектор демонструє слайд 40

Сайт про безпечний онлайн-шопінг від OLX - ОНЛАЙН(ЗА)ХИСТ
https://safety.olx.ua/



Тут є все, щоб поліпшити твою кіберграмотність. Читання будь-якого матеріалу займе не більше кількох хвилин. Обов'язково застосовуйте отримані знання, щоб не дати шахраям жодного шансу.

Тут можна почитати реальні історії про онлайн-шахрайство та пройти тести на перевірку своїх знань.

Лектор демонструє слайд 41

Сайт НБУ з платіжної безпеки #ШахрайГудбай

https://promo.bank.gov.ua/stopfraud/

#ШахрайГудбай – це інформаційна кампанія, мета якої навчити українців правилам безпеки безготівкових та онлайн-платежів. У межах цієї кампанії Національний банк створив сайт із правилами платіжної безпеки.

На сайті ви знайдете більше інформації про:

- телефонне шахрайство та сценарії шахрайства,
- лайфхаки безпечних онлайн-покупок та онлайн-шопінгу,
- ознаки листів від шахраїв та шахрайських сайтів.

Також на сайті розміщені відеоролики та постери з актуальними сценаріями шахрайства.

Електронне навчальне видання
План-конспект уроку з фінансової грамотності
для учнів старшої школи на тему:
"Поради з кібербезпеки та схеми шахрайства
у воєнний час"

Укладач: Машлаковська Тетяна
Літературний редактор: Кладіна Тетяна
Травень 2022 року

Національний банк України
01601 м. Київ
вул. Інститутська, 9
https://bank.gov.ua/

Відгуки, пропозиції та зауваження
надсилайте на електронну адресу: finlit@bank.gov.ua