Національний
банк України

ПЛАН-КОНСПЕКТ
уроку з фінансової грамотності "Правила платіжної безпеки. Види шахрайства"
для учнів середньої школи

ЗМІСТ

Тема уроку: "Правила платіжної безпеки. Види шахрайства"

Мета уроку: навчити учнів правил платіжної безпеки, познайомити з видами та сценаріями шахрайства, щоб уберегти учнів від таких випадків.

Терміни, про які учні дізнаються під час уроку: фішинг, вішинг, скімінг.

Розгорнутий план уроку

1. Хто такі шахраї?

- Шахраї, які фізично крадуть гроші.
- Шахраї у віртуальному світі.
- Хто ловить шахраїв?

2. Вид шахрайства "фішинг".

- Що таке "фішинг"?
- Куди шахраї надсилають посилання?
- Приклад фішингу "Повідомлення від друзів".
- Приклад фішингу "Повідомлення від друзів про допомогу".

3. Платіжна банківська картка.

- Які реквізити картки можна повідомляти, а які ні?

4. Вид шахрайства "вішинг" (телефонне шахрайство).

- Що таке "вішинг"?
- Як вберегтися від вішингу?

5. Вид шахрайства "скімінг".

- Що таке "скімінг"?
- Як безпечно знімати готівку з банкомата?

6. Смартфон та методи захисту смартфона від шахраїв.

- Чому важливо оберігати смартфон від шахраїв?
- Паролі та біометрія для захисту смартфона.
- Налаштування сповіщень на заблокованому екрані.
- Смартфон має бути під наглядом.
- Що робити, якщо втратив смартфон?

7. Паролі: як створити складні та унікальні паролі.

- Якими мають бути паролі до акаунтів?
- Поради для створення паролів.

8. 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:

- як уберегтися від таких видів шахрайства: фішинг, вішинг, скімінг;
- яку інформацію про платіжну картку можна повідомляти, а яку ні;
- як правильно знімати готівку з банкомата;
- як захисти свої смартфони;
- як створити складний та надійний пароль.

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

Конспект уроку

Питання 1. Хто такі шахраї?

Лектор демонструє слайди 1-2

Привітання, знайомство та інформування про тему заняття.

Доброго дня, дорогі учні.

Лектор демонструє слайд 3

Сьогодні ми будемо говорити про шахраїв та правила платіжної безпеки, які допоможуть вберегти свої кошти.

Шахрай – це та людина, яка шляхом обману інших людей намагається привласнити чужі кошти.

Лектор демонструє слайд 4

Раніше шахраї намагалися красти кошти в реальному світі, наприклад, шляхом зламу сейфа чи крадіжки гаманця з грошима.

Лектор демонструє слайд 5

З потужним розвитком сучасних технологій та використанням людьми безготівкових розрахунків шахраї змінили своє поле діяльності та почали вигадувати способи крадіжки коштів у віртуальному світі. Щоб не потрапити у пастку шахраїв, потрібно використовувати прості правила платіжної безпеки, які ми сьогодні з вами детально розглянемо.

Лектор демонструє слайд 6

Як шахраї діють у віртуальному просторі? Один із способів, коли вони видають себе за інших осіб та випитують у людей секретну інформацію про їх платіжні картки, логіни та паролі. Ця інформація дає змогу шахраю отримати доступ до безготівкових коштів та викрасти їх. Щоб цього не трапилося, потрібно знати, яку інформацію в жодному разі не можна нікому повідомляти. Ким може представитися шахрай? Насправді, будь-ким:

- вашим другом;
- працівником поліції;
- працівником банку;
- працівником НБУ, Пенсійного фонду, Фіскальної служби;
- працівником комунальних служб;
- працівником мобільного оператора.

І цей перелік невичерпний.

Наприклад, шахрай може зателефонувати людині, представитися працівником банку, повідомити, що з її картки крадуть гроші і, щоб запобігти крадіжці просять повідомити секретну інформацію про картку, яка надає доступ до її грошей.

Людина, перебуваючи в стані страху через потенційну втрату коштів, може повідомити зайву інформацію.

Питання для аудиторії: Чи стикався хтось із ваших близьких із випадками шахрайства?

(відповіді дітей)

Друзі, дякую вам за відповіді.

Лектор демонструє слайд 7

Звісно, дії шахраїв є незаконними. І за таку діяльність вони обов'язково несуть покарання. Пошуком таких шахраїв займається Кіберполіція. Це Департамент Національної поліції України. Про випадки шахрайства необхідно повідомляти Кіберполіцію, щоб шахраїв могли знайти та покарати.

Питання 2. Вид шахрайства "фішинг".

Лектор демонструє слайд 8

Шахраї в своїх злочинних схемах використовують різні методи та підходи, тому існують різні види шахрайства, які ми з вами зараз детально розглянемо.

Перший вид шахрайства, про який ми з вами будемо говорити – це фішинг.

Фішинг (у перекладі з англ. означає "риболовля") – це вид шахрайства в інтернеті, що дає змогу шахраям виманити особисту інформацію про людину та незаконно заволодіти її коштами.

У фішингу є кілька різновидів. Наприклад, шахраї можуть створювати сайти, які візуально схожі на сайти відомих брендів, банків, магазинів тощо.

Адреси справжнього та шахрайського сайтів можуть бути схожі, за винятком одного чи кількох символів.

Тому потрібно завжди перевіряти правильність назви сайтів, на які переходите та вводите свої персональні дані, логіни та паролі.

Якщо необхідно перейти за посиланням на сайт компанії, адресу якого ви отримали в повідомленні, введіть у пошуковій системі назву необхідного сайту і лише тоді переходьте на вебресурс.

Лектор демонструє слайд 9

Шахраї можуть надсилати шкідливі посилання:

- у месенджер;
- смс-повідомленням;
- на e-mail.

Навіщо шахраї розсилають шкідливі посилання?

Для "зараження" пристроїв вірусом або викрадення персональних даних, секретних карткових реквізитів.

Наприклад, в умовах воєнного стану з'явилася схема шахрайства, коли шахраї розсилають смс-повідомлення про те, що людині зарахована грошова допомога, деталі за посиланням, зазначаючи шахрайське посилання.

<u>Питання до аудиторії: Чи стикалися ви чи ваші батьки з таким видом шахрайтва як фішинг?</u>

(відповіді дітей)

Друзі, дякую вам за відповіді.

Лектор демонструє слайд 10

Розглянемо ще приклади фішингу.

Шахраї від імені друзів можуть надсилати повідомлення з різним змістом, які містять шахрайські посилання, метою яких може бути: зараження вірусом вашого пристрою або крадіжка персональних даних, карткових реквізитів, отримання доступів до ваших акаунтів у соціальних мережах.

Приклад такого повідомлення ви бачите на слайді.

Привіт,
Це ти на відео? ☹
https://www.ofkfk/uk/

Лектор демонструє слайд 11

Як не потрапити на "гачок" шахрая?

Не поспішайте переходити за посиланням.

Спочатку думайте – потім клікайте!

Не переходьте за посиланнями від незнайомців.

Якщо отримали посилання від друга, не поспішайте за ним переходити.

Шахраї могли отримати доступ до акаунта друга. Спершу зателефонуйте йому та запитайте, чи справді посилання від нього.

Лектор демонструє слайд 12

Розглянемо ще один сценарій шахрайства.

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.

Лектор демонструє слайд 13

Що робити, якщо отримали таке повідомлення?

Звичайно, подібна ситуація може статися з кожним, друг дійсно міг опинитися в скрутному становищі.

Але перш ніж позичати гроші:

- запитайте друга про те, що можете знати тільки ви і він. Таке питання одразу викриє шахрая;
- перетелефонуйте другові на номер, 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 адреси усіх підписників зламаної сторінки.

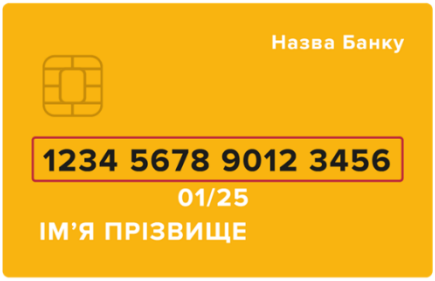
Також під час війни стали відомі випадки, коли шахраї зламують сторінки в соціальних мережах, наприклад у фейсбуці, потім роблять публікацію на сторінці її власника та від його імені просять про фінансову допомогу на купівлю амуніції у зв'язку з відбуттям на фронт.

Питання 3. Платіжна банківська картка

Лектор демонструє слайд 14

За допомогою платіжної картки можна оплачувати за товари в магазинах, купувати онлайн. Безготівкові розрахунки – це дуже зручно й швидко. Але, щоб гроші не дісталися шахраям і їм не вдалося їх вкрасти з платіжної картки, потрібно дотримуватися простих правил та знати, яку інформацію про платіжну картку можна повідомляти, а яку ні.

Не можна розголошувати всі реквізити платіжної картки.

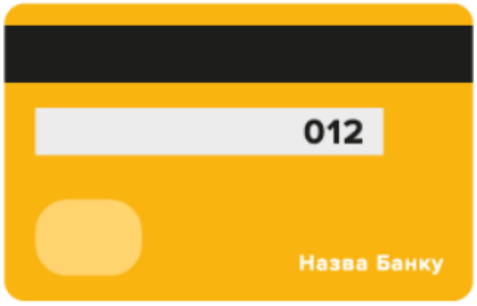


16-значний номер картки – єдине, що можна повідомляти. Цю інформацію повідомляти безпечно, її достатньо для того, щоб на картку перерахували гроші.

Є інформація, яку в жодному разі не можна нікому повідомляти.

Це три цифри на звороті картки та термін дії картки. Якщо телефоном просять повідомити три цифри на звороті картки – це перша ознака шахрайства.

Справжній працівник банку ніколи не запитає таку інформацію.



Питання 4. Вид шахрайства "вішинг".

Лектор демонструє слайд 15

Розглянемо наступний вид шахрайства вішинг або телефонне шахрайство.

Вішинг – це вид шахрайства, коли шахрай телефонує і переконує людину повідомити секретну інформацію або переказати гроші.

На яку інформацію полює шахрай?

- Інформацію про платіжну картку.
- Паролі.
- Коди в смс, які надсилають банки.

Лектор демонструє слайд 16

Пам’ятайте, шахрай може назватися будь-ким: працівником банку чи поліції. Якщо телефонують та запитують про вашу платіжну картку, краще бути не ввічливим та покласти слухавку. Повідомте батьків про випадок, у разі потреби батьки зв’яжуться з банком.

Сценаріїв телефонних розмов шахраїв не один десяток, про один із них ми говорили на початку уроку. Але мета таких розмов одна – виманити секретну інформацію, яка надасть змогу шахраям вкрасти гроші.

Питання 5. Вид шахрайства "скімінг".

Лектор демонструє слайд 17

Ми з вами говорили про те, що не можна повідомляти три цифри на звороті картки та термін дії картки. Також не можна повідомляти пін-код. Пін-код – це чотири секретні цифри, які знає лише власник картки. Пін-код видається власнику картки під час її отримання в банку в закритому конверті, навіть працівник банку його не знає. Пін-код потрібен, наприклад, для зняття готівки в банкоматі, іноді під час оплати карткою товарів у магазині.

Розглянемо наступний вид шахрайства, який називається "скімінг".

Питання для аудиторії: діти можливо ви чули про такий вид шахрайства та знаєте що він означає?

(відповіді дітей)

Друзі, дякую вам за відповіді.

Лектор демонструє слайд 18

Отже, скімінг – це вид шахрайства, коли шахрай робить копію платіжної картки за допомогою спеціального обладнання, яке встановлює на банкомат.

Лектор демонструє слайд 19

Але для того, щоб вкрасти гроші шахраю також необхідний пін-код. Щоб його дізнатися, шахрай установлює маленьку, майже непомітну, камеру на банкомат.

Лектор демонструє слайд 20

Через відеокамеру, шахрай підглядає, який пін-код вводить людина.

Лектор демонструє слайд 21

Але уникнути такого шахрайства дуже просто. Потрібно дотримуватися простого правила.

Лектор демонструє слайд 22

Під час користування банкоматом потрібно правильно прикривати його клавіатуру під час уведення пін-коду, а саме: однією рукою прикриваєте, а іншою натискаєте на клавіатуру.

Також потрібно пильнувати, щоб той, хто стоїть позаду в черзі до банкомата, не бачив, як ви вводите пін-код. Якщо людина стоїть в черзі до банкомата, потрібно тримати відстань від тієї людини, яка вже знімає готівку. Це є правило ввічливої поведінки, щоб людина, яка вводить пін-код, не хвилювалася, що його хтось побачить.

Питання 6. Смартфон та методи захисту смартфону від шахраїв.

Лектор демонструє слайди 23-24

У наш час смартфон є не лише засобом для зв’язку з друзями та близькими.

Смартфон містить багато цінної інформації, особисті фото, фото документів. Через смартфон ми заходимо до акаунтів у соціальних мережах, електронної пошти тощо. Ця інформація, якщо потрапить до рук шахрая, може бути використана в злочинних цілях. Ставтеся до свого смартфона, як до гаманця, не залишайте його без нагляду. Смартфон потрібно пильнувати та берегти як зіницю ока.

Наприклад, шахраї через смартфон можуть зайти на сторінку в соціальних мережах та попросити допомоги в друзів від імені власника

сторінки. І це лише один із багатьох варіантів, як шахраї можуть скористатися чужим смартфоном.

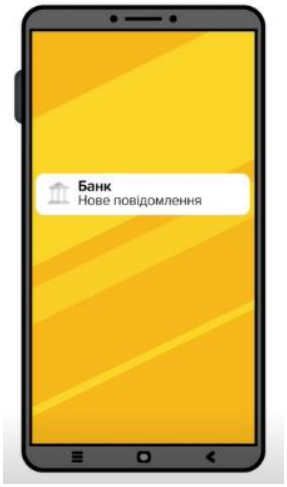
Лектор демонструє слайди 25

Отже, як 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.

Лектор демонструє слайди 26

Налаштуйте показ сповіщень на заблокованому екрані у такий спосіб, щоб ховати їх конфіденційний вміст, як це показано на слайді.



Налаштуйте цю функцію самостійно або попросіть допомоги в дорослих.

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

Лектор демонструє слайди 27

Не залишайте смартфон без нагляду, завжди його тримайте біля себе.

Лектор демонструє слайд 28

Що робити, якщо втратили смартфон?

1. Негайно повідомте батьків.

2. Змініть паролі на тих ресурсах, якими користувалися через смартфон або попросіть допомоги в дорослих.

Якщо смартфон опинився в руках шахрая, швидка зміна паролів до акаунтів завадить йому отримати доступ до них через ваш смартфон.

Питання 7. Паролі – як створити складні та унікальні паролі.

Лектор демонструє слайд 29

Також є шахраї, які вміють зламувати акаунти, підбирати до них паролі. Для того, щоб їм це не вдалося необхідно створювати складні та унікальні паролі.

Памятайте, що пароль – це ключ до ваших даних. Не можна недооцінювати його значення, важливо приділяти цьому питанню значну увагу.

Який пароль уважається складним та надійним?

Складний пароль може містити:

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

Лектор демонструє слайд 30

Для створення паролів не використовуйте імена домашніх улюбленців, свої хобі, дату народження тощо. Також не можна використовувати для паролів загальновідомі комбінації паролів (наприклад, Qwerty12, Password123456, Admin1234 тощо), послідовне/зворотне написання символів або цифр.

Лектор демонструє слайд 31

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 спецсимволи, за тільки вам відомою системою.

Лектор демонструє слайд 32

Тримайте в секреті паролі, їх не можна розповідати навіть друзям. Також не варто їх записувати. Паролі потрібно завчити на зубок.

Лектор демонструє слайд 33

Паролі мають відрізнятися!

Пам'ятайте! Пароль має бути унікальним для кожного акаунта: електронної пошти, соціальної мережі, персонального кабінету на сайті інтернет-крамниці тощо.

Якщо просунутий зловмисник отримає доступ до вашого пароля з інтернет-крамниці, то він може спробувати той самий пароль до електронної пошти або до акаунта в соціальних мережах.

Злочинці користуються тим, що люди, як правило, використовують однакові або схожі паролі.

Питання 8. Ресурси для учнів для поліпшення власних навичок із платіжної безпеки.

Лектор демонструє слайд 34

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

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

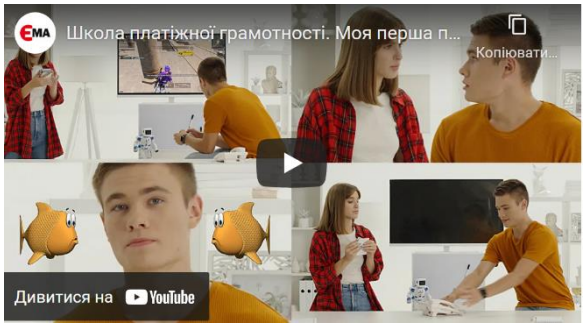
Антишахрайська онлайн-гра "Здолай шахрая", розроблена Асоціацією "ЄМА", покликана допомогти громадянам розвивати й поліпшувати власні навички з кібербезпеки та захисту від більше ніж 80 видів платіжного та інтернет-шахрайства!

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 35

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?

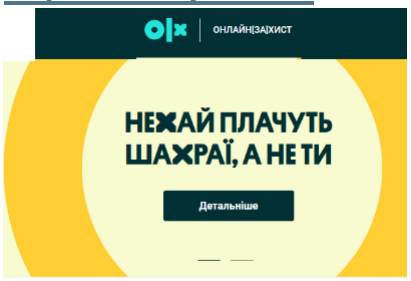
Про сучасні платіжні технології:

- як самостійно та швидко оформити платіжну картку,
- як оплатити купівлю товарів смарт-годинником чи смартфоном,
- як безпечно розраховуватися в інтернеті,
- як перевіряти платіжні сайти.

Тільки живі приклади без нудного пояснення.

Лектор демонструє слайд 36

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



Тут є все, щоб посилити 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 37

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 середньої школи на тему:
"Правила платіжної безпеки. Види шахрайства"

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