Національний банк України

ПЛАН-КОНСПЕКТ
заняття з платіжної безпеки "Поради з кібербезпеки та схеми шахрайства у воєнний час"

для учнів старшої школи та студентів

ЗМІСТ

- Розгорнутий план та загальна інформація про заняття.
- Поради з кібербезпеки у воєнний час.
- Актуальні схеми шахрайства у воєнний час.
- Правила безпечних онлайн-покупок.
- Телефонне шахрайство.
- Фінансовий номер телефону.
- Ресурс для учнів/студенів для поліпшення власних навичок із платіжної безпеки.

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

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

Терміни, про які учні/студенти дізнаються під час заняття: фінансовий номер телефону, багатофакторна автентифікація.

Розгорнутий план заняття

1. **Поради з кібербезпеки у воєнний час.**
- Як захистити кошти на платіжній картці?
- NFC у смартфонах чи безпечно користуватися?
- Як захистити акаунти та смартфони?
- Правила, яких потрібно дотримуватися, при скануванні QR-кодів.

2. **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.

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.
- Телефонні дзвінки шахраїв від імені працівників банків.
- Що робити, якщо на зв'язку шахрай?

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

6. **Ресурс для учнів/студентів для поліпшення власних навичок із платіжної безпеки.**
- Сайт НБУ з платіжної безпеки #ШахрайГудбай.

7. Самостійна робота учнів/студентів з робочим зошитом. Після виконання учнями/студентами завдань педагог з учнями/студентами обговорюють результати практичної роботи та її аналізують.

Після завершення заняття учні/студенти 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 заняття учні/студенти 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.

Конспект заняття

Питання 1. Поради з кібербезпеки у воєнний час.

Педагог демонструє слайди 1-2

Привітання, знайомство та інформування про тему заняття.

Доброго дня!

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

(відповіді).

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.

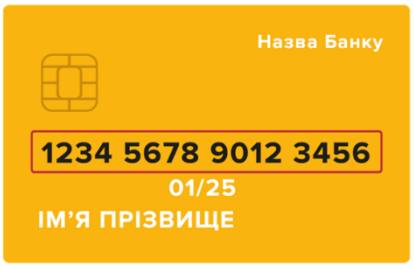
Питання для аудиторії: А чи знаєте ви, яку інформацію про платіжну картку можна повідомляти стороннім особам?

(відповіді).

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.

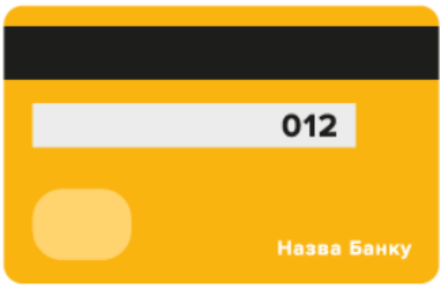


Педагог демонструє слайд 3

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.

Педагог 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.

Педагог 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.

Педагог 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.

Педагог демонструє слайд 8

Змінюйте пін-код до картки:

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

Педагог демонструє слайди 9-10

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.

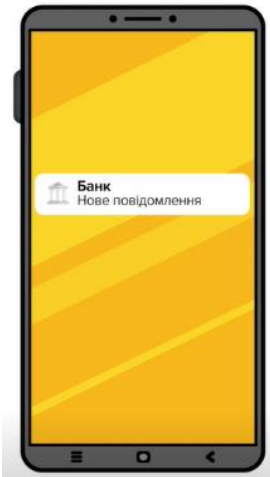
Face ID — це спосіб автентифікації через розпізнавання обличчя.

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

Педагог демонструє слайди 11

Захистіть ваш смартфон, адже на вашому смартфоні багато цінної інформації, яку можуть використати шахраї, дотримуйтеся наступних порад:

- встановіть пароль на вхід / використовуйте біометричні дані для входу;
- налаштуйте сповіщення на заблокованому екрані у такий спосіб, щоб ховати їхній конфіденційний вміст;
- змініть заводський PIN-код до SIM-картки на стійкий (8-значний);
- використовуйте лише ліцензійні програми, мобільні застосунки та систематично їх оновлюйте.



У випадку втрати смартфону або його крадіжки, спочатку потрібно зателефонувати до мобільного оператора, а потім до банку, щоб заблокувати свої рахунки.

Педагог демонструє слайд 12

Є кілька ефективних способів захисту акаунтів у соціальних мережах:

- складний та унікальний пароль;
- багатофакторна автентифікація.

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

Педагог демонструє слайд 13

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.

Педагог демонструє слайд 14

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.

Педагог демонструє слайд 15

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.

Педагог демонструє слайд 16

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.

Педагог демонструє слайди 17

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.

Педагог демонструє слайд 18

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.

Педагог демонструє слайд 19

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.

Педагог демонструє слайд 20

QR-коди використовують у різних сферах життя. Їх можна побачити на плакатах, упаковках товарів. У музеях біля експонатів часто розміщують таблички з QR-кодами, відксанувавши їх, можна дізнатися більше про експонат. У кафе та ресторанах за QR-кодом можна ознайомитися з меню. За допомогою такого коду підтверджується купівля залізничних квитків. Також QR-коди активно використовують для безготівкових розрахунків.

На жаль, за QR-кодами можуть бути зашифровані як і безпечні, так і шахрайські посилання. Тому до QR-кодів, як і до посилань, потрібно ставитися обережно.

При скануванні QR-кодів дотримуйтеся таких правил:

- скануйте QR-коди тільки із перевірених джерел, утримайтесь 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.

Питання 2. Актуальні схеми шахрайства у воєнний час.

Педагог демонструє слайд 21

Розглянемо актуальні у воєнний час сценарії шахрайства.

Шахраї зламують облікові записи в соціальних мережах та месенджерах (Facebook, Instagram, Telegram). Для цього поширюють фішингові посилання, наприклад, під виглядом пропозицій взяти участь у голосуванні, конкурсі, пропозицій роботи в інтернеті тощо. Перейшовши за посиланнями, громадяни вводять логіни та паролі від своїх акаунтів у соціальних мережах/месенджерах, які автоматично стають відомі шахраям.

Далі шахраї від імені власника акаунту розсилають підписникам однакові повідомлення такого змісту: "Привіт! Позич, будь ласка, гроші до завтра! Дуже треба!".

Суму шахраї зазначають різну, вказують номери своїх карток, таким чином привласнюють кошти осіб, які погоджуються їх позичити.

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

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.

Педагог демонструє слайд 22

Можливий також і інший варіант цієї схеми:

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.

Щоб запобігти зламу акаунтів у соціальних мережах та месенджерах необхідно:

- створювати складні та унікальні паролі для кожного акаунту;
- налаштовувати двофакторну автенфікацію всюди, де це можливо;
- не переходити за сумнівними посиланнями;
- тримати в секреті свої логіни та паролі;
- не вводити свої логіни та паролі від акаунтів на незнайомих та підозрілих вебсайтах.

Перш ніж ввести логін та пароль – перевірте URL-адресу необхідного ресурсу, адже будь-які відмінності можуть вказувати на те, що ви опинилися на фішинговому сайті. Також рекомендується додатково перевірити безкоштовно сайт на шахрайство на:

- ✓ сайті Кіберполіції у розділі "STOP FRAUD": https://cyberpolice.gov.ua/stopfraud/;
- ✓ сервісі Асоціації "ЄМА" CheckMyLink: https://check.ema.com.ua/.

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.

Педагог демонструє слайд 23

Розглянемо наступний сценарій шахрайства. Щоб ошукати громадян та викрасти кошти з їхніх карток, шахраї можуть використовувати таку технологію, як спуфінг (підробка).

Спуфінг – це ситуація, 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. Тобто людині телефонує чи пише шахрай, а на екрані гаджета відображається український номер банку, пенсійного фонду, податкової, поліції тощо.

Наприклад, шахраї можуть використовувати спуфінг для підміни номера телефону та імітувати смс та дзвінки від банків. Роботизований голос під різними приводами повідомляє про необхідність надання банківських конфіденційних даних фейковому працівникові банку. Отримавши ці відомості, зловмисники привласнюють кошти.

Щоб уникнути подібного шахрайства:

- **нікому не повідомляйте:**
  - ✓ смс-коди від банків;
  - ✓ три цифри на звороті картки (CVV-код);
  - ✓ логіни та паролі від інтернет-банкінгу.

Справжні працівники банків ніколи не запитують конфіденційних даних у клієнтів;

- **телефонуйте банку за номером, зазначеним на звороті платіжної картки.**

Педагог демонструє слайд 24

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, зокрема єПідтримки, допомоги від ЄС, представників ООН, Червоного Хреста, різних програм благодійних фондів. У розсилках шахраї пропонують перейти за посиланням та вказати дані банківських карток, на котрі нібито буде зарахована допомога.

Також зловмисники створюють шахрайські сайти, схожі на справжні сайти державних органів, міжнародних організацій, банків та благодійних фондів.

Громадяни переходять за посиланням, бачать сайт, схожий на справжню сторінку відповідної організації, вводять усі дані, які автоматично стають відомі шахраям.

Маючи дані банківських карток громадян, вони привласнюють гроші з рахунків.

Педагог демонструє слайди 25-26

Щоб уникнути подібного шахрайства:

- **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. Перш ніж ввести в будь-яку форму дані своєї платіжної картки або паролі до онлайн-банкінгу – перевірте URL-адресу необхідного ресурсу, адже будь-які відмінності можуть вказувати на те, що ви опинилися на фішинговому сайті. Також рекомендується додатково перевірити безкоштовно сайт на шахрайство на:

✓ сайті Кіберполіції у розділі "STOP FRAUD": https://cyberpolice.gov.ua/stopfraud/;
✓ сервісі Асоціації "ЄМА" CheckMyLink: https://check.ema.com.ua/.

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.

Педагог 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.

Шахраї також надсилають смс-повідомлення від імені банку про те, що з рахунку громадянина намагаються зняти кошти. Якщо переказ особа не здійснювала, потрібно зателефонувати «псевдобанку» за номером, зазначеним в смс, або перейти за посиланням.

Якщо особа переходить за посиланням, то потрапляє на шахрайський сайт, де під виглядом блокування шахрайської трансакції й автоматичного повернення грошей пропонується ввести:

- номер телефону;
- пароль до інтернет-банкінгу;
- всі реквізити карти;
- смс-код (код підтвердження проведення операції).

Якщо особа телефонує за вказаним в смс номером телефону, шахрай веде жертву на цей самий шахрайський сайт, де схиляє ввести вищезазначені дані.

Питання 3. Правила безпечних онлайн-покупок

Педагог демонструє слайд 28

Розглянемо схему шахрайства, коли шахраї на торговельних майданчиках представляються продавцями.

Шахрайська схема така: покупець знаходить потрібний товар на торговельному майданчику (наприклад, OLX) та виходить на зв'язок із продавцем, який насправді є шахраєм.

Псевдопродавець замість того, щоб обговорювати деталі угоди в особистому кабінеті торговельного майданчика, несподівано пропонує перейти в месенджер, де продовжується листування стосовно товару.

Псевдопродавець може надсилати додаткові фото товару і підтримувати розмову про товар. Коли приходить час платити, шахрай надає посилання для оплати, яке веде на фішинговий сайт.

Вже на фішинговому сайті покупець вводить реквізити картки: номер, термін дії, тризначний код CVV та код із смс (підтвердження операції). Шахрай отримує цю інформацію та краде гроші з картки покупця.

Педагог демонструє слайд 29

Як розпізнати псевдопродавця?

Ознаки псевдопродавця:

- поспішає з оплатою;
- виманює секретні реквізити картки;
- переводить спілкування з особистого кабінету на сайті оголошень у месенджер;
- просить зняти ліміт із картки для проведення оплати.

Педагог демонструє слайд 30

Щоб купувати онлайн безпечно, потрібно дотримуватися простих правил:

- **не переходьте в месенджери, коли купуєте на торговому онлайн-майданчику/дошці оголошень:**
  - ✓ обговорюйте деталі угоди виключно в чаті платформи або використовуючи додаток платформи;
  - ✓ не реагуйте, якщо вам пропонують спілкуватися в месенджерах (Viber, Telegram, WhatsApp);
- **надавайте перевагу післяплаті.** Остерігайтеся рекламних оголошень, які заманюють купити якісні речі за мінімальними цінами;
- **не переходьте за посиланнями від незнайомців.** Спершу перевірте адресу, тільки потім клацайте на посилання;
- **не вводьте реквізитів платіжних карток на незнайомих та підозрілих вебсайтах.**

Перш ніж ввести в будь-яку форму дані своєї платіжної картки або паролі до онлайн-банкінгу – перевірте URL-адресу необхідного ресурсу, адже будь-які відмінності можуть вказувати на те, що ви опинилися на фішинговому сайті. Також рекомендується додатково перевірити безкоштовно сайт на шахрайство на:

✓ сайті Кіберполіції у розділі "STOP FRAUD": https://cyberpolice.gov.ua/stopfraud/;

✓ сервісі Асоціації "ЄМА" CheckMyLink: https://check.ema.com.ua/.

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.

- завжди тримайте в секреті: тризначний номер на звороті картки, коди банків, паролі до інтернет-банкінгу.

Питання 4. Телефонне шахрайство.

Педагог 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.

Педагог 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;
- 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.

Педагог демонструє слайд 33

Дуже поширеним сценарієм шахрайства лишаються телефонні дзвінки від імені працівників банків. Шахраї телефонують та представляються працівниками служби безпеки банку та виманюють у громадян конфіденційну інформацію про їхні картки та рахунки, що потім дає можливість привласнити кошти громадян.

Під час таких телефонних розмов шахрай може:

варіант 1 – запевняти, що до рахунків громадянина отримали доступ сторонні. Надалі шахрай випитує фінансові дані нібито для запобігання шахрайству, однак, отримавши ці відомості, привласнює гроші;

варіант 2 – просити громадянина надати інформацію про картки та рахунки через планову перевірку даних у зв'язку з війною; отримавши ці відомості, привласнює гроші;

варіант 3 – повідомляти про кібератаку на ІТ-систему банку та просити перерахувати гроші на тимчасовий безпечний рахунок, який насправді є рахунком шахрая;

варіант 4 – просити встановити програму віддаленого доступу для посилення заходів безпеки. Якщо громадянин виконує вказівки, шахрай отримує віддалено доступ до його онлайн-банкінгу та від імені громадянина перераховує кошти на інший рахунок.

Педагог 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).

Друзі, дякую вам за відповіді.

Питання 5. Фінансовий номер телефону.

Педагог 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.

Педагог демонструє слайд 36

Приклад схеми крадіжки фінансового номера телефону.

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.

Педагог 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. Ресурс для учнів/студентів для поліпшення власних навичок із платіжної безпеки.

Педагог демонструє слайд 38

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 заняття з платіжної безпеки
для учнів старшої школи та студентів на тему:
"Поради з кібербезпеки та схеми шахрайства
у воєнний час"

Укладач: Машлаковська Тетяна
Літературний редактор: Кладіна Тетяна
Березень 2023 року

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

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