МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРКУТУРНИЙ ПІДРОЗДІЛ
«КОСТЯНТИНІВСЬКИЙ ІНДУСТРІАЛЬНИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

МЕТОДИЧНІ ВКАЗІВКИ

«Кібербезпека: навички, які захищають не тільки під час війни».

для проведення виховної години

студентів закладів фахової передвищої освіти

Розроблено:
Викладачем
ВСП КІФК ДВНЗ ДонНТУ
першої категорії
Журавель Г.Ю.

Луцьк - 2022

Тема: «Кібербезпека: навички, які захищають не тільки під час війни».

Мета виховної години — продемонструвати приклади загроз в інтернеті та пояснити, як можна їх уникнути й захистити свої дані. При цьому задача не налякати та відмовити студентів від ведення блогів, поширення сторіз, знайомств через інтернет тощо. Але важливо до кожної дії в інтернеті підходити критично та відповідально, дотримуватися певних правих, і тоді перебування у віртуальному просторі не буде загрозливим.

Завдання виховної години:

- пояснити небезпеки публікації / надання доступу до особистих даних / локації телефону в загальному доступі;
- навчити ідентифікувати ознаки фішингу;
- дати розуміння важливості захисту акаунтів;
- запропонувати дієві кроки для убезпечення своїх персональних даних та поради щодо загальної безпеки онлайн.

Чи замислювалися ви над тим, хто має доступ до інформації, яку ви публікуєте в соцмережах або шукаєте в інтернеті? Наскільки надійним є захист вашого профілю? Чи знаєте ви, що таке фішинг і як захиститися від нього? Від початку повномасштабного вторгнення Росії в Україну відповіді на ці та інші запитання набули нового значення, бо стали асоціюватися із захистом не тільки віртуального, але й реального життя. Нам може здаватися, що ми, як звичайні користувачі інтернету, не цікавимо кіберзлочинців, а отже й не потребуємо додаткових знань із кібербезпеки. Проте за допомогою мережі ми спілкуємося, працюємо, навчаємося, купуємо товари та послуги, здійснюємо різні банківські операції, шукаємо інформацію тощо. Відповідно, ми можемо бути мішенню інтернет-шахраїв. Тому знання правил безпеки в інтернеті допоможуть захистити персональні дані та убезпечити фінансові дії в інтернеті. Вміння ж захистити свої персональні дані в умовах війни може навіть вберегти чиєсь життя.

Структура виховної години:

Етап І. Мотиваційний. Чому нам потрібна кібербезпека?

Етап ІІ. Практичний. Аналізуємо приклади в мінігрупах.

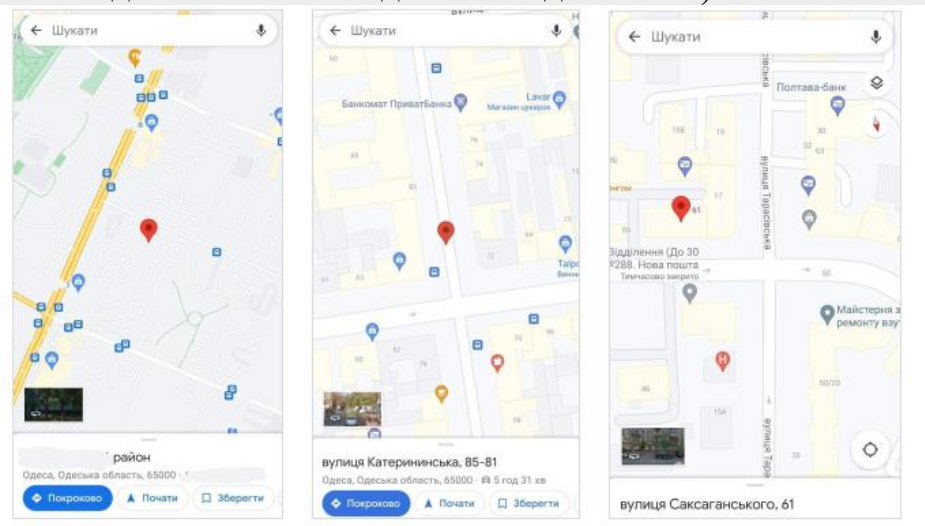
Етап ІІІ. Домашнє завдання. Добираємо рекомендації щодо безпеки в інтернеті для однолітків і батьків.

ЕТАП I. Мотиваційний. Чому нам потрібна кібербезпека?

Здобувачам освіти необхідно переглянути декілька реальних прикладів з інтернету й пояснити, які небезпеки можуть приховувати такі публікації або повідомлення.

Приклад 1. Студентам необхідно уважно подивитися на зображення та назвати, що спільного між ними (скоріше за все вони здогадаються та назвуть геотег, геолокацію, відмітку місця). ЗАПИТАЙТЕ. Чи вбачаєте ви якісь загрози в тому, що у сторіз або на фото підлітки можуть ставити геотеги (геотег, або геолокація вказує на місце розташування конкретного об’єкта на онлайн-мапі)?

Якщо так, то які? (Вислухайте варіанти відповідей та попросіть їх пояснити. Спробуйте наштовхнути студентів на роздуми про публічність такої інформації, про те, хто бачить такі повідомлення, — чи обмежують вони їх своїм найближчим колом друзів чи дозволяють бачити всім користувачам. Чи повідомляють вони свою домашню адресу або адреси пересування містом усім, із ким знайомі, при спілкуванні наживо? Чи не виглядали би такі повідомлення дивними?)



Спочатку студенти мають назвати, що спільного у скриншотах, зробити припущення щодо можливих загроз. Після цього демонструється зображення карт, які з'явились би, якщо натиснути на значок геотегу з попередніх зображень. Таким чином підтверджується припущення студентів або показується, в чому може бути небезпека. Тобто, якщо дивитися на перші скриншоти, то вони виглядають звичайно та звично для підлітків, а якщо перейти за геотегом та поєднати інформацію про відпустку чи новенький ноутбук з інформацією про адресу, то небезпека стає зрозумілою.

На всіх запропонованих зображеннях спільною рисою є відмітка про розташування — геотег. При натисканні на нього відкриється онлайн-карта з точною адресою. Навіть на зображенні, де використано популярний геотег «Там, де живе любов».

Геотег є зручною функцією, яка допомагає сортувати фото, повідомити, де ви перебуваєте, та спростити пояснення того, як до вас дістатися. Проте варто пам'ятати не тільки про зручності, а й про небезпеки, які може приховувати публікація такої інформації. Маючи профіль у будь-якій із соціальних мереж, ви так чи інакше привернете увагу т. зв. мережевих шпигунів або переслідувачів (англ. social stalkers). Ці сучасні «шкідники» (англ. modern creepers) використовують публічну інформацію та з легкістю можуть дізнатися вашу адресу, захоплення, улюблені місця перебування та інше. Тож невинна публікація про те, що вас не буде вдома впродовж тижня, бо ви летите у відпустку, повідомить усім, хто має змогу це побачити, що ваш дім / квартира пустує. З огляду на те, що багатьох своїх підписників підлітки можуть не знати особисто й навіть ніколи не зустрічати в реальному житті, то вони не можуть бути певні, що серед цих людей не буде мережевих шпигунів.

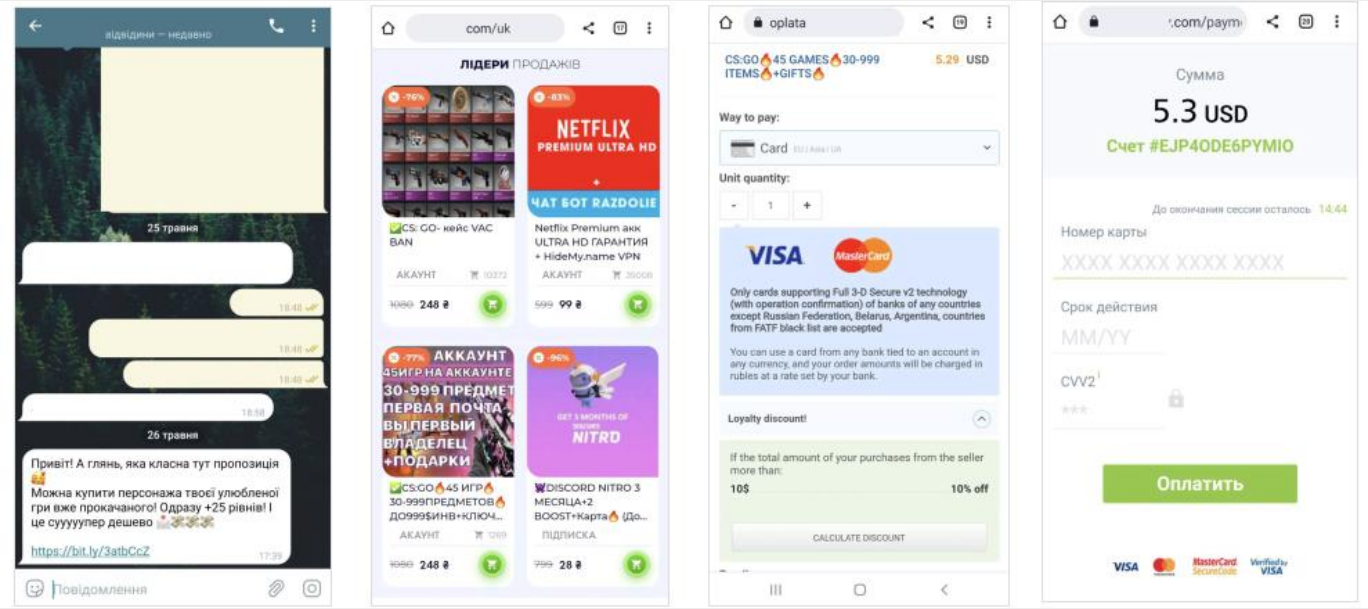
Якщо ви мрієте стати блогером/-кою, варто пам'ятати, що велика кількість чутливої інформації у вільному доступі може нашкодити. Ми ніколи не дізнаємося, хто і як використає дані, які викладаємо в інтернет. Особливо в часи, коли Україна перебуває в активній фазі захисту своїх територій від агресії Росії. Кожен із нас, пересічних користувачів інтернетом, може бути об'єктом відстеження. Тож варто бути обачними. Важливо розуміти, що будь-яка публічна відвертість може нашкодити людям, із якими ви живете: батькам, сестрам / братам та іншим. Особливо якщо, окрім геотега, ви ще пишете якусь приватну інформацію про своїх близьких.

Бажання детально описувати своє життя може мати непередбачувані наслідки й зачіпати близьких людей (батьків) або тих, кого стосується поширена інформація. Під чутливою інформацією варто розуміти не тільки геотег, а й надмірну відвертість. Проте це не значить, що не варто нічого писати в мережі. Це радше заклик свідомо ставитися до інформації. Перед тим як щось запостити в соціальних мережах, запитайте себе: чи не нашкодить ця інформація мені та моїм близьким?

Подумайте, чи варто всім користувачам знати про це й чи не варто обмежити це коло, наприклад, тільки близькими друзями та родиною.

Приклад №2. Передивитись скриншот із повідомленням про можливість отримати покращеного героя в інтернет-грі за мінімальну вартість. Для цього потрібно перейти за покликанням.

Чи не викликає це повідомлення сумнівів? Якщо так, то що саме?



Сайт виглядає начебто надійно, схожий на вже наявний майданчик для продажу різних онлайн-ігор, але ціну пропонує набагато нижчу за ту, яка є на верифікованому майданчику.

Дуже спокуслива пропозиція. І купити все можна за спрощеною системою — лише ввести номер картки, CVV2 код, не потрібно ніякої реєстрації, сайт і так дізнається, який у вас акаунт у грі й завантажить все одразу в профіль. Які можуть бути наслідки таких дій? Чому ця пропозиція підозріла?

Це один із популярних методів соціальної інженерії — фішинг. Соціальна інженерія в інформаційній безпеці — це спосіб атаки, який використовує не технічні вразливості системи, а особливості людської психіки — страхи, зацікавленість або довіру.

Фішинг (від англійського слова fishing — риболовля) — це атака, спрямована на те, щоб користувач сам видав шахраям щось важливе або ж завантажив шкідливе програмне забезпечення, яке збиратиме дані чи пошкодить систему. Зазвичай зловмисники полюють за так званими обліковими даними (наприклад, дані для входу в акаунти: електронна пошта, пароль або код) чи грошима.

У цьому випадку шахрай хоче, щоб користувач/-ка, який/яка спокуситься акцією, ввів/-ла номер карти й код (можливо, карти батьків, якщо це дитина) та дав/-ла зловмиснику доступ до грошей. Звичайно, після цього сайт стягне максимально можливу суму й ніяких послуг не надасть.

На що варто звертати увагу, щоб не стати жертвою фішингу:

- ✓ емоційність повідомлення — це може бути обіцянка виграшу, чогось дешевого / доступного. Або гра на соромі, на страху щось заблокувати / втратити;

- ✓ вимога діяти швидко — фішинг спонукає нас ухвалювати рішення швидко, не даючи часу на роздуми, а отже й не дозволяючи поставитися до отриманої інформації критично;
- ✓ непередбачуваність — ця атака може мати будь-яку форму і статися на будь-якій платформі. Це може бути лист на електронну пошту, смс, повідомлення в месенджері, пост в інстаграмі.

Додатково про фішинг:
https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html
https://www.naiau.kiev.ua/news/yak-ne-stati-zhertvoyu-kartkovih-shahrayiv.html

Якщо ви отримали повідомлення, яке викликає сильні емоції і спонукає до термінової дії, перше, що варто зробити: зупинитись і подумати, що ви бачите. Потім дослідити (бажано з людиною, яка може дати фахову пораду), що ви отримали, і вже на підставі критичної оцінки ухвалювати рішення.

Не варто спокушатись на першу-ліпшу пропозицію, особливо якщо сайт просить у нас доступ до фінансів. Якщо ви маєте дозвіл на витрачання грошей або на користування карткою від батьків, то краще зайти на офіційний сайт гри напряму.

Досить часто, на жаль, люди вважають, що кібербезпека стосується тільки спеціалістів. Проте, як ви могли переконатися, прості правила поведінки в інтернеті стосуються кожного користувача й можуть убезпечити наш віртуальний простір та фінанси. Щоб іще більше переконатися в цьому,

ЕТАП ІІ. Практичний. Аналізуємо приклади в мінігрупах.

Цей етап проводиться двома способами: із груповою роботою в мінігрупах або зі спільним обговоренням кожного кейсу.

Варіант 1 (групова робота)

Об’єднуємо студентів в чотири групи (за кількістю кейсів, які пропонуються для аналізу) та пропонуємо їм перейти до онлайн-обговорення.

Учасників/-ць груп повинні фіксувати свої міркування та аргументи на стікерах і кріпити їх на онлайн дошці. По завершенню обговорення, яке триватиме 5 хв, представник/-ця групи має презентувати результат обговорення.

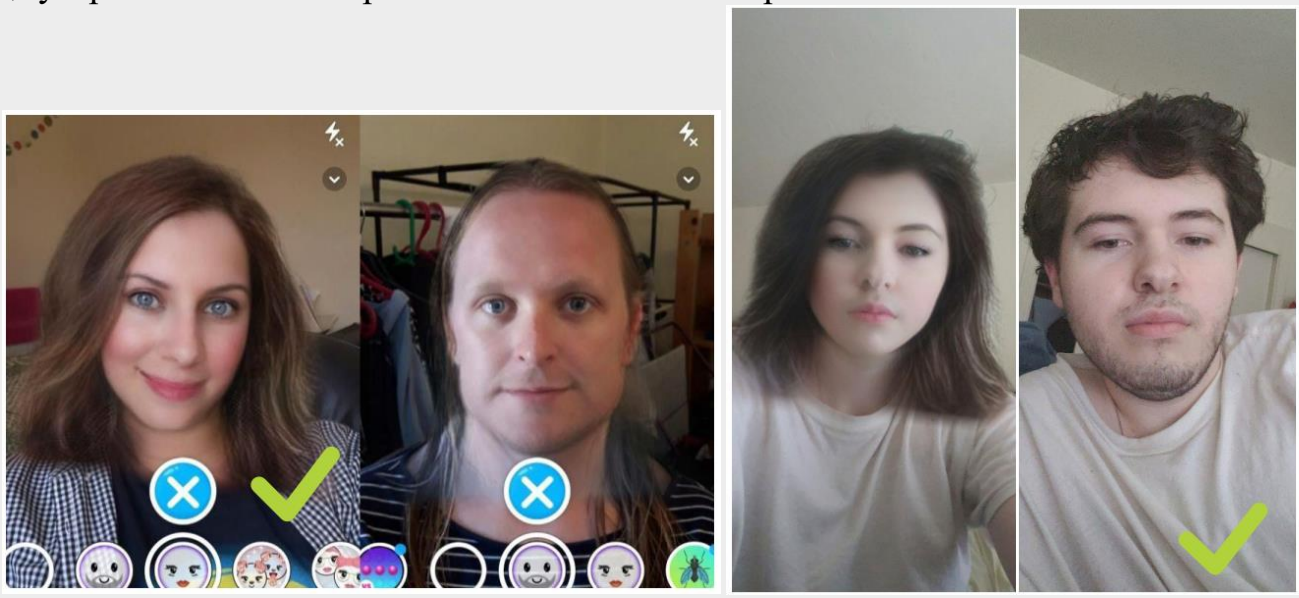
Варіант 2 (спільне обговорення)

Почергово демонструється відповідний слайд із презентації або дошку на Jamboard, студенти повинні вмикати мікрофони і висловлювати свої припущення. Тим, хто соромиться говорити, мають можливість писати свої думки в чаті або на стікері (якщо працюєте з Jamboard).

Кейси для аналізу

Кейс 1.

Ваш/-ша друг/подруга познайомився/-лася в інтернеті з привабливою дівчиною/хлопцем. Спілкуються вже декілька місяців на різні теми. І от новий знайомий/-ма запропонував/-ла зустрітися. Що ви порадите: зустрітися, відмовитися від зустрічі або інший варіант? Поясніть свій вибір.



Після того, як група представить результати обговорення.

Треба запитати: Чи замислювалися ви над тим, що можете листуватися з людиною, яка не буде тою/тим, за кого себе видає? Що вона може старшою / молодшою, іншої статі й зовнішності?

Демонструються приклади фото, на яких можна побачити докорінну зміну зовнішності, використовуючи фотофільтри.

Як ви гадаєте, на якому з пари фото зображена реальна людина? (У першому випадку жінка, а у другому чоловік, використовуючи фотофільтри, змінили свою зовнішність.)

Сам по собі факт онлайн-спілкування не є поганим. Але треба бути впевненим/-ою, що ви спілкуєтеся справді з тією людиною, а не з фейком або з людиною, яка не є тією, за кого себе видає. Наприклад, набагато старша за віком або не тієї статі про, яку пише.

Дуже просто зробити фотографію зі зміненою зовнішністю й навіть статтю (Для кращого розуміння теми рекомендуємо ознайомитися з іншим уроком від проєкту «Віртуальний та реальний світи: чи є ежа?»). Як ми бачимо на фотографіях, для цього достатньо декількох кліків у додатку — і зовнішність змінюється за допомогою спеціальних фільтрів. Також важливо розуміти, що й онлайн-спілкування може бути токсичним та погано впливати на психічне здоров’я. Тому до нього також, як і до реального, варто ставитися критично.

На що звертати увагу при спілкуванні онлайн:

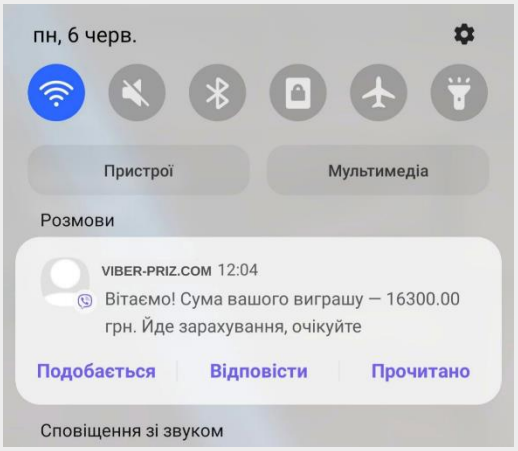
- Чи уникає людина спілкування по відео або відмовляється надсилати актуальні фотографії, де добре видно обличчя (є ризик, що людина не та, за кого себе видає). Важливо! Порада щодо надсилання свого фото стороннім особам допустима, зважаючи на контекст. Тобто, якщо ви спілкуєтеся тривалий час онлайн і плануєте зустрітися в реальності, то прохання про актуальне фото є нормальним. В інших ситуаціях не варто надсилати своє фото незнайомій людині.
- Чи просить гроші на будь-які потреби (лікування хвороб, допомогу, форс-мажорні обставини тощо).
- Чи залишає після спілкування відчуття провини за те, що ви з кимось пішли гуляти / щось робити / просто пішли з онлайну займатися справами. Такі відчуття є ознакою токсичного спілкування, якого краще уникати.
- Чи вимагає розкрити чутливу інформацію (школу, де ви навчаєтесь, домашню адресу, інформацію про батьків та їхнє місце роботи, просить надсилати відверті фотографії).Якщо хоча б на один із пунктів ви дали ствердну відповідь, то варто уважно поставитися до нового/-ої знайомого/-ої.

Як уберегтися від неприємних наслідків:

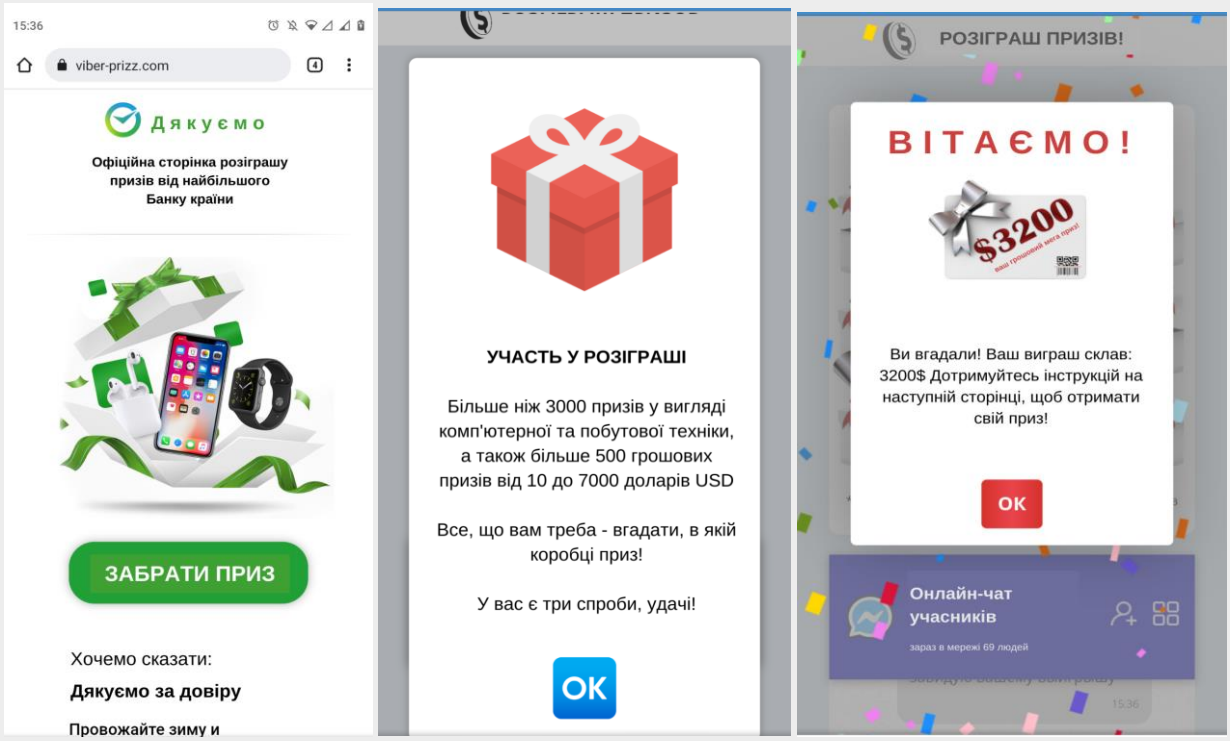
- ✓ Попросіть перед зустріччю поспілкуватись по відеозв'язку (це допоможе зрозуміти, чи правда перед вами та людина, з якою ви познайомилися).
- ✓ Повідомте батьків або інших дорослих, яким ви довіряєте, про свою майбутню зустріч.
- ✓ Оберіть для зустрічі публічне людне місце, яке ви добре знаєте. За жодних обставин НЕ погоджуйтесь на зустріч у безлюдному місці, квартирі, машині та в іншому закритому просторі наодинці.
- ✓ Домовтеся про зустріч безпосередньо в обраному місці (краще не погоджуватися на спільний похід до місця зустрічі).

Кейс 2.

Ваш/-ша молодший/-ша брат/сестра отримав/-ла у вайбері повідомлення про виграш значної суми грошей. Для отримання виграшу потрібно перейти за лінком та дізнатися подробиці. Що ви порадите: перейти за лінком, проігнорувати або щось інше? Поясніть свій вибір.

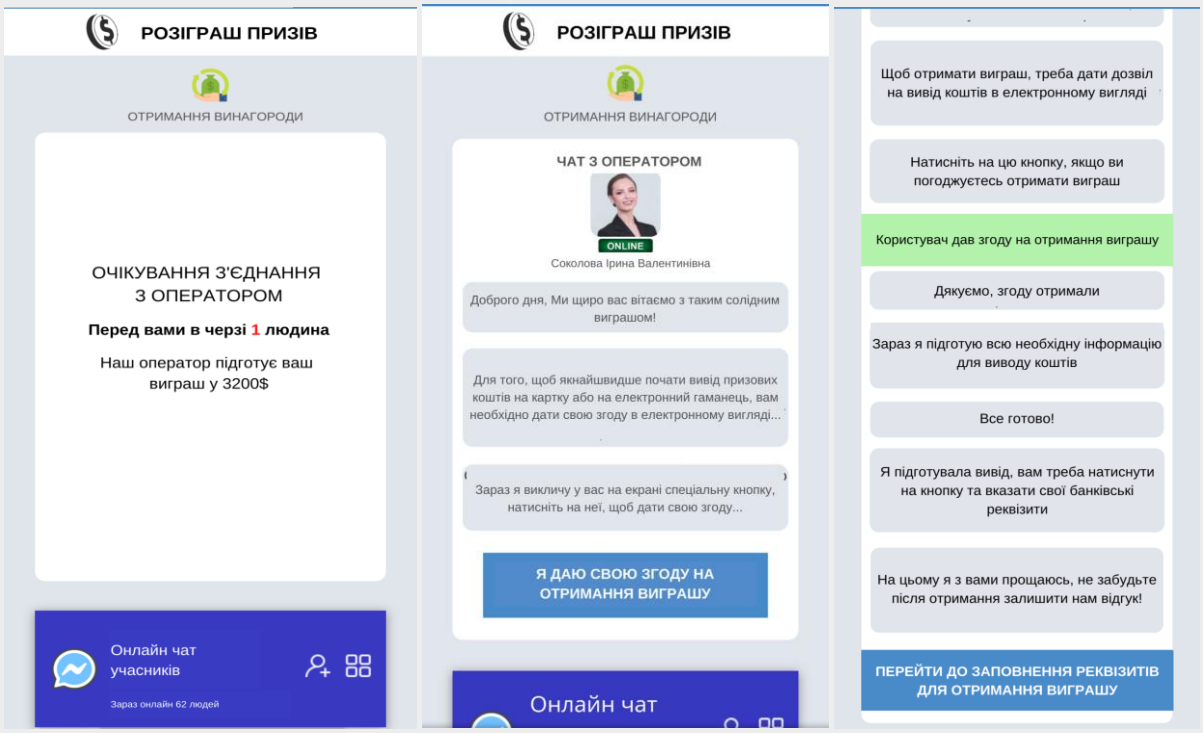


Коли ви перейдете за покликанням, то опинитеся на сайті начебто з розіграшем від «найбільшого банку країни» рис.2. Якщо натиснути «забрати приз», то ви потрапите на сторінку, де треба відгадати, в якій коробці ховається «приз» рис. 3,4



Вже з першої спроби ви виграєте (рис. 5), і вам запропонують зв’язатися з оператором.

Оператор запропонує натиснути на згоду отримати виграш (рис. 6, 7), а потім уже попросить перейти на сторінку для введення реквізитів. Там вам запропонують ввести номер карти, строк її дії та CVV2 код. Після чого зловмисник матиме змогу списати наявні на картці кошти.



Перед вами був іще один приклад фішингу. Звичайно, що виграш фейковий і цю інформацію в мережі розмістили для виманювання реальних даних користувачів. Важливо наголосити, що не можна повідомляти номер карти, її строк дії та CVV2 код, бо таким чином зловмисники не нарахують гроші, а спишуть ті, що є на картці.

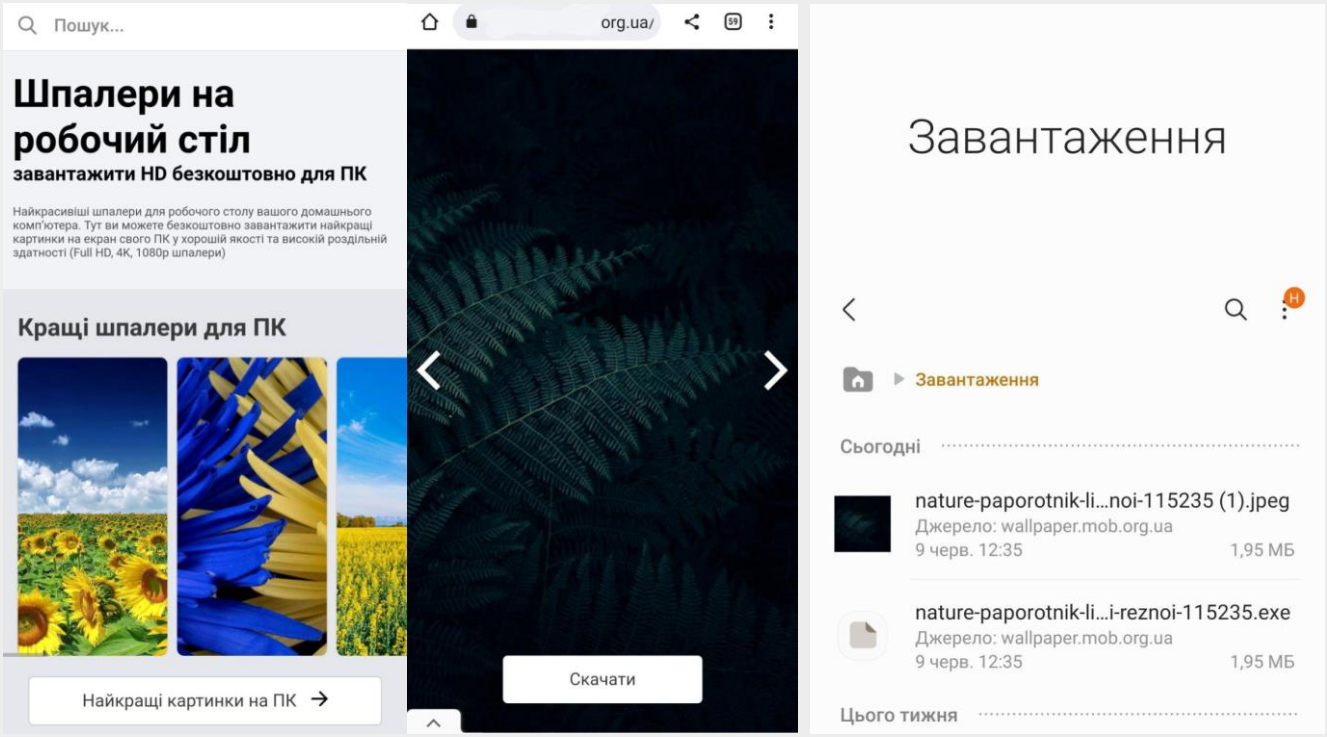
При використанні банківської картки для оплати в інтернеті важливо:

1) купувати тільки на перевірених сайтах, що починаються з https:// або позначені зображенням закритого замочка біля інтернет-адреси сайта;
2) виконувати операції оплати лише на захищеному комп'ютері з обмеженим доступом до нього сторонніх осіб — не використовуйте для здійснення розрахунків комп'ютери загального призначення в загальних місцях або комп'ютери сторонніх осіб;
3) не забувати своєчасно оновлювати операційну систему та антивірусні програми;
4) остерігатися фішингових сайтів. Перелік відомих фішингових сайтів можна переглянути на сайті Української міжбанківської асоціації членів платіжних систем ЄМА;
5) ніколи не вводити PIN-код в інтернет! Для оплати покупок достатньо лише ввести:
   - ✓ номер картки;
   - ✓ термін її дії;
   - ✓ CVV2/CVC2-код;
   - ✓ одноразовий пароль (якщо сайт підтримує технологію 3D-Secure). Пароль із sms-повідомлення від банку — додатковий «поріг» безпеки, який є в картках, захищених за системою 3D Secure. Він надсилається на телефонний номер, закріплений за вашим картковим рахунком. Це дозволяє додатково убезпечити картку від шахрайських посягань;
6) перевірити, чи не внесений вебресурс до «Чорного списку шахрайських сайтів» Української міжбанківської асоціації членів платіжних систем ЄМА;
7) не довіряти занадто привабливим пропозиціям. Не існує сервісів, які безкоштовно надають послуги!
8) Скористатися «Білим списком надійних сервісів» від Асоціації ЄМА.

Кейс 3.

Ви шукали нове зображення, щоб оновити шпалери головного екрана комп'ютера або телефона. Після завантаження ви з'ясували, що, окрім самого зображення, завантажився ще exe-файл. Що ви зробите: видалите його, відкриєте чи щось інше? Поясніть свій вибір.

Іноді з потрібним файлом у мережі можна завантажити щось шкідливе, особливо якщо шукати й завантажувати не з офіційних джерел розповсюдження / перевірених сайтів. Якщо вже припустилися помилки й завантажили файл, важливо не клікати на нього й не встановлювати, бо за файлом «зображення.exe» може ховатись вірус, який нашкодить комп'ютеру та інформації на ньому.



Чому так відбувається? Для того щоб ви могли завантажити картинку або файл, людям треба вкласти певний ресурс у розробку сайта, його підтримку та обслуговування, а також наповнення контентом.

Якщо якась послуга пропонується безкоштовно для користувача, можливо, власник сервісу отримує кошти з чогось іншого. Це може бути розміщення рекламних банерів на сайті, продаж певної інформації про користувачів, які користуються сервісом, або «реалізація» шкідливого програмного забезпечення. Якщо власник сервісу користується останнім сценарієм, то радше за все разом із файлом ви завантажите собі на пристрій певну програму («вірус»), яка тим чи іншим чином нашкодить вашому девайсу. До прикладу, це може бути програма-шифрувальник, яка заблокує вам доступ до вашого ж пристрою та вимагатиме грошей за його розблокування.

Не можна завантажувати підозрілі файли, а користуватись слід тільки перевіреними сервісами. Також варто звертати увагу на файли з розширенням .exe, .bat, .apk (на телефоні), .cmd, .wsf. Такі файли мають певний сценарій взаємодії з комп'ютером. Після їхнього запуску на пристрій може бути встановлено шкідливе програмне забезпечення.

Щоб уникнути такої небезпеки, потрібно:

- користуватися перевіреними сервісами;
- не завантажувати підозрілі додатки на телефон в обхід офіційних маркетів (Google Play, App Store);
- не запускати та не встановлювати підозрілий файл, якщо завантаження його відбулося.

Кейс 4.

Ваш/ -а друг / подруга має сторінку в інстаграмі. Щодня викладає сторіз на різні теми та має позитивні реакції на них від підписників, яких стає більше. Одного дня друг / подруга в розпачі повідомляє, що його / її сторінку зламали й він / вона не має до неї доступу. Звернувшись на форум техпідтримки, ін / вона отримав / отримала різні поради й тепер просить вас допомогти обрати потрібні. Можна обрати декілька варіантів та обґрунтувати свій вибір.

Перелік порад:

- ✓ створити новий пароль, який ви легко запам’ятаєте;
- ✓ переслати пароль кращій другу / подрузі в повідомленні, щоб точно до нього був доступ;
- ✓ налаштувати двофакторну автентифікацію;
- ✓ заходити у свої акаунти з чужих пристроїв тільки за крайньої потреби та не забувайте потім виходити;
- ✓ якщо у вашого акаунту пароль складний та надійний, то можна його використовувати і для інших сервісів, включаючи банківську картку;
- ✓ можна не виходити з акаунту на чужому телефоні, щоби в разі чого мати доступ до профілю;
- ✓ не обов’язково налаштовувати двофакторну автентифікацію, якщо пароль надійний;
- ✓ створити складний та надійний пароль більше чотирьох знаків, який включатиме заголовні букви, цифри та символи.

Скоріше за все, в хлопця / дівчини стояв дуже простий пароль, який зловмисник міг із легкістю підібрати. Важливо пам’ятати, що акаунти, які мають для нас цінність, треба налаштувати добре, а саме:

- поставити довгий та складний пароль;
- налаштувати двофакторну автентифікацію;
- пам’ятати, що варто виходити з акаунтів на чужих пристроях;
- не розголошувати важливу інформацію, яка стосується банківських карток;
- не використовувати однаковий пароль для кількох акаунтів.

Витік може статися, наприклад, на сайті кінотеатру, де ви зареєструвалися через те, що інакше не можна купити квиток. І там не варто використовувати свій пароль для пошти, соцмереж, банкінгу та інших важливих сервісів. Зламавши слабко захищений сайт кінотеатру, зловмисники отримають доступ не лише до його бази даних, а й до пошти чи соцмереж користувачів, які використовують однакові паролі для цих сервісів. Також потрібно розуміти, що, отримавши доступ до вашої сторінки, зловмисники отримають доступ і до вашої переписки. Таким чином небезпека втратити чутливу інформацію є не тільки у вас, а у всіх ваших онлайн-співрозмовників.

Використовувати тільки пароль для захисту акаунту недостатньо. Важливо встановлювати двофакторну автентифікацію (2ФА). Тобто для входу потрібен пароль і ще щось, зазвичай це коди.

Таким чином, навіть якщо зловмисники мають ваш пароль, вони не зможуть зайти у ваш акаунт без коду. Найважливіше, що потрібно знати про 2ФА:

- ❖ важливо зберегти коди відновлення і про них не забути;
- ❖ це не панацея, але вона значно зменшить імовірність зламу;
- ❖ на месенджери вона теж потрібна (другий фактор у месенджерах — це пароль).

Двофакторна автентифікація — додатковий рівень захисту для вашого облікового запису на випадок, якщо зловмисник якимось чином дізнається (підгляне, вгадає тощо) ваш пароль.

Вона передбачає, що при вході в обліковий запис із нового пристрою та браузера фейсбук / інстаграм / твітер, окрім пароля, вимагатиме додаткового підтвердження вашої ідентичності. Таким підтвердженням може бути:

- ▪ sms з одноразовим кодом;
- ▪ додаток для смартфона (iOS або Android), який автоматично генеруватиме такі коди;
- ▪ набір із десяти одноразових резервних кодів, які ви можете роздрукувати чи переписати у блокнот;
- ▪ фізичний ключ безпеки, який треба вставляти в USB-порт, наприклад, YubiKey.

Якщо зловмисник знає ваш пароль, не маючи другого фактора (якогось із перерахованих вище), він не зможе зайти у ваш обліковий запис. І навпаки: маючи лише другий фактор, зловмисник не отримає доступу до вашого облікового запису — йому потрібно буде також дізнатися ваш пароль.

Більше можна почитати тут: https://yak.dslua.org.

ЕТАП ІІІ. Домашнє завдання. Добираємо рекомендації для однолітків та батьків.

Всі приклади, з якими ми працювали впродовж заняття, були взяті з реального життя. Всі учасники сьогоднішнього заняття є пересічними користувачами інтернету, які не надавали значення безпеці в інтернеті. Ігноруючи ці правила, люди стають жертвами фішингу, сталкінгу, зламу акаунту та втрачають свої дані.

Пропоную підсумувати все, про що ми з вами говорили впродовж уроку. Для цього вам потрібно буде вдома виконати завдання.

ДОМАШНЄ ЗАВДАННЯ:

Сформулюйте топ п’ятірку порад із кібербезпеки для своїх однолітків, батьків та молодших братів / сестричок. Поясніть, чому ви поставили те чи інше правило на перше місце для конкретної групи (однолітки, батьки, молодші брати / сестри). Які з

порад ви відкинули й чому. Для складання топу скористайтеся списком порад, який склали експерти з кібербезпеки.

Список порад:

- Використовуйте довгий та складний пароль для захисту своїх акаунтів.
- Налаштуйте двофакторну автентифікацію.
- Пам’ятати, що варто виходити зі своїх акаунтів, якщо ви зайшли на чужому пристрої.
- Не завантажуйте підозрілі додатки на телефон в обхід офіційних маркетів (Google Play, App Store).
- Користуйтеся тільки перевіреними інтернет-сервісами.
- Не запускайте та не встановлюйте підозрілий файл, якщо його завантаження відбулося.
- Не розголошуйте важливої інформації, яка стосується банківських карток.
- Звертайте увагу на сайт, на якому плануєте використати банківську картку для оплати.
- Уникайте занадто емоційних повідомлень — це може бути обіцянка виграшу, чогось дешевого / доступного.
- Ставтеся критично до вимог діяти швидко.
- Будьте обережними щодо прохань про фінансову допомогу від малознайомих людей в інтернеті.
- Звертайте увагу, чи не уникає новий/-ва інтернет-знайомий/-ма спілкування по відео або відмовляється надсилати актуальні фотографії, де добре видно обличчя (є ризик, що людина не та, за кого себе видає).
- Перевіряйте, чи не залишаються у вас після спілкування онлайн відчуття провини за те, що ви з кимось пішли гуляти / щось робити / просто пішли з онлайну займатися справами. Такі відчуття є ознакою токсичного спілкування, якого краще уникати.
- Не розкривайте чутливу інформацію в інтернеті (школу, де ви навчаєтесь, домашню адресу, інформацію про батьків та їхнє місце роботи).
- Нікому не надсилайте відверті фотографії.

Найголовніше, що ви повинні запам’ятати з нашого заняття, — це те, що ми не закликаємо вас припинити користуватися інтернетом. Навпаки, ми хочемо наголосити на критичному ставленні до всієї інформації, яку ви отримуєте, та на дотриманні простих правил, які допоможуть убезпечити вас, ваші дані та фінанси від інтернет-шахраїв.

ДЖЕРЕЛА:

1. Національний проєкт з медіаграмотності Міністерства культури та інформаційної політики України – Фільтр. — Режим доступу до ресурсу: https://filter.mkip.gov.ua/uchytelyam-ta-uchnyam/
2. Гудима В. Чому не можна використовувати один пароль для всіх акаунтів? [Електронний ресурс] / В. Гудима, М. Капранова // ЯК? — 2021. — Режим доступу до ресурсу: https://yak.dslua.org/articles/chomu-ne-mozhna-vykorystovuvaty-odyn-parol-dlia-vsikh-akauntiv/
3. Двофакторна автентифікація [Електронний ресурс] // ЯК? — 2021. — Режим доступу до ресурсу: https://yak.dslua.org/services/facebook/2fa/
4. Капранова М. Ловися, рибко: як інтернет-шахраї ошукують користувачів [Електронний ресурс] / Мар'яна Капранова // Куншт. — 2021. — Режим доступу до ресурсу: ної оплати банківською картою у мережі Інтернет [Електронний ресурс] // Банк «Південний» — Режим доступу до ресурсу: https://bank.com.ua/internet-safety
5. Правила безпечної оплати банківською картою у мережі Інтернет [Електронний ресурс] // Банк «Південний» — Режим доступу до ресурсу: https://bank.com.ua/internet-safety
6. Савчук Т. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті [Електронний ресурс] / Тетяна Савчук // Радіо Свобода. — 2018. — Режим доступу до ресурсу: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.
7. Сомова О. Розширення для перекладу у браузері. ТОП-8 сервісів для Google Chrome [Електронний ресурс] / Ольга Сомова // Webpromo. — 2022. — Режим доступу до ресурсу: https://web-promo.ua/ua/blog/rasshireniya-dlya-perevoda-v-brauzere-top-8-servisov-dlya-google-chrome/
8. Як не стати жертвою «карткових» шахраїв [Електронний ресурс] // Національна академія внутрішніх справ. — 2016. — Режим доступу до ресурсу: https://www.naiau.kiev.ua/news/yak-ne-stati-zhertvoyu-kartkovih-shahrayiv.html
9. The Risks in Geo Tegging [Електронний ресурс] // Safe Online. — Б.р. — Режим доступу до ресурсу: https://safeonline.ng/social-media/understanding-the-risks-in-geo-tagging/
10. https://mon.gov.ua/ua/ministerstvo/diyalnist/mizhnarodna-dilnist/spivpracya-z-mizhnarodnimi-organizaciyami/rada-mizhnarodnih-naukovih-doslidzhen-ta-obminiv-irex/programa-vivchaj-ta-rozriznyaj-infomedijna-gramotnist

ПРИМІТКА. Усі зображення, використані на занятті, були взяті з відкритих джерел.