Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ЕКОЛОГО-НАТУРАЛІСТИЧНИЙ ЦЕНТР УЧНІВСЬКОЇ МОЛОДІ
04074. Київ, Вишгородська, 19 Тел. 430-02-60, 430-43-90 e-mail: nenc@nenc.gov.ua

«05» грудня 2022 р. № 213

Директорам закладів
позашкільної освіти
еколого-натуралістичного
напряму

Щодо інформаційного захисту
в закладах позашкільної освіти

Інформаційно-методичний матеріал
«Абетка інформаційного захисту позашкілля»

Високий рівень комп'ютеризації вимагає дотримання певних правил поведінки для убезпечення себе та оточення від загроз в інформаційній сфері.

Кіберборотьба та протидія кіберзагрозам в інформаційній сфері розглядається сучасним суспільством будь-якої країни як один із найважливіших пріоритетів безпеки.

Заклади освіти вразливі до загроз кібербезпеці здебільшого через кількість пристроїв, якими вони керують, різноманітність операційних систем, тощо. Кібербезпека є важливою темою для всіх, а не лише для корпорацій. Здобувачам освіти закладів ПО також важливо розуміти, як залишатися в безпеці в Інтернеті.

Експерти з кібербезпеки рекомендують всім закладам освіти створити власну команду з кібербезпеки, а також застосувати деякі ключові найкращі практики для забезпечення безпеки та конфіденційності.

Чому кібербезпека важлива в освіті?

Важливість кібербезпеки в закладах освіти постійно зростає. Інтернет і комп’ютери стали невід’ємною частиною нашого повсякденного життя, незалежно від того, працюємо ми чи навчаємося вдома.

Тому дуже важливо захистити комп’ютери та Інтернет від неавторизованих людей, щоб інформація, яка є цінним активом будь-якого закладу освіти, залишалася в безпеці.

Типи загроз кібербезпеці в закладах освіти

1. Основні типи загроз кібербезпеці в закладах позашкільної освіти включають фішинг, зловмисне програмне забезпечення, програми-вимагачі, спам, соціальна інженерія та атаки на відмову в обслуговуванні. Кіберзлочинці використовують ці засоби для націлювання на заклади освіти з метою отримання фінансової вигоди.
2. Фішинг – це найпоширеніша форма кібератак, яка використовується кіберзлочинцями для злому систем закладів освіти.
3. Інший спосіб, яким фішери можуть спробувати отримати доступ до вашої системи, – це інсталювати шкідливе програмне забезпечення на вашому комп’ютері. Зловмисне програмне забезпечення – це програма або файл, який заражає вашу систему та може викрасти конфіденційну інформацію.
4. Спам — це ще один спосіб, за допомогою якого кіберзлочинці можуть отримати доступ до вашої системи, розсилаючи спам-повідомлення зі шкідливими посиланнями або вкладенням.
5. Спам-лист часто виглядає як офіційне повідомлення від закладу освіти чи компанії з проханням до користувачів оновити свою особисту інформацію, натиснувши посилання або завантаживши вкладений файл, який заразить їхню систему шкідливим програмним забезпеченням і вірусами, якщо вони потраплять у пастку.
6. Спам-повідомлення також використовуються кіберзлочинцями для розповсюдження вірусів та інших форм зловмисного програмного забезпечення через заражені файли, вкладені у спам-повідомлення.

Список викликів кібербезпеці в освітньому секторі

Незахищені бездротові з’єднання: використання бездротових з’єднань стало дуже поширеним у сучасному світі. Однак існує потреба у захисті цих бездротових з’єднань. Незахищені бездротові з’єднання можуть бути легко зламані хакерами, що може призвести до крадіжки та порушення даних.

Бездротові маршрутизатори: багато закладів освіти не піклуються про свої бездротові маршрутизатори або не встановлюють брандмауер на своїх

маршрутизаторах, що робить їх уразливими до кібератак з боку зовнішніх хакерів або навіть внутрішніх працівників, яким доручено керувати мережевою інфраструктурою закладу освіти. Це також призводить до витоку та крадіжки.

Соціальні медіа, які стали дуже популярними. Тому існує потреба обмежити доступ до таких сайтів, як Facebook і Twitter, у робочий час.

Що таке знання кібербезпеки для учнів?

Кібербезпека – це сфера освіти, яка розвивається. Оскільки багато учнів щодня мають доступ до Інтернету, то у кіберзлочинців є багато можливостей викрасти паролі чи особисту інформацію. Навчання з питань кібербезпеки є важливим, оскільки воно навчає учнів, як вони можуть захистити себе від кібератак. Вони дізнаються про фішингові шахрайства, зловмисне програмне забезпечення, програми-вимагачі та інші комп'ютерні загрози.

Заклади освіти повинні захистити себе від хакерів, встановивши брандмауери, захист від зловмисного програмного забезпечення та інші засоби захисту. Бажано переконатися, що всі пристрої, підключені до її мережі Wi-Fi, захищені надійними паролями.

Важливо, щоб діти мали безпечний спосіб досліджувати світ, не боячись бути атакованими в Інтернеті, тому такі програми, як KidsZone, були створені, щоб допомогти захистити дітей від кіберзалякування.

Чому обізнаність про кібербезпеку важлива?

Програми поінформованості про кібербезпеку мають бути обов'язковими в закладах освіти, щоб кожен міг навчитися залишатися в безпеці в Інтернеті. Більшість хакерів мотивуються викликом, а не фінансовою винагородою. Якщо хакер зможе привернути вашу увагу, він зможе проникнути у вашу систему.

Заклади освіти є однією з найбільш уразливих цілей для кібератак, оскільки вони мають великі мережі комп'ютерів і часто не забезпечують дотримання необхідних протоколів.

Найбільша проблема кіберпростору така: у пересічних громадян є відчуття, що у випадку загрози вони можуть просто розв'язувати цю проблему, вимкнувши телефон чи комп'ютер. Утім, ця думка – хибна. Тож ми маємо розуміти правила поведінки в кіберпросторі та навчитися з цим жити:

- Встановлюйте надійний пароль, не коротший за 12 символів, із використанням прописних літер, цифр та інших знаків. Чим довший і складніший пароль, тим менша ймовірність витоку конфіденційної інформації в Інтернет.
- Номера свого телефону, номер близьких Вам людей, адреса, номер ідентифікаційного коду – ПОГАНІ ідеї для паролю.
- Не записуйте своїх паролів, не зберігайте їх поруч із ноутбуком, мобільним телефоном чи банківськими картами.
- Не зберігайте паролі у браузері, навіть якщо це зручно. Один такий крок і усі зможуть отримати ваші данні.
- Використовуйте різні паролі для кількох облікових засобів або сервісів.
- Не надсилайте особистої інформації, користуючись WI-Fi у публічному місці.
- Не здійснюйте банківських операцій онлайн, використовуючи публічний WI-Fi.
- Виходьте зі своїх профілів, якщо Ви користувалися публічним комп'ютером.
- Вимикайте комп'ютер, якщо надовго йдете зі свого робочого місця.
- Не завантажуйте файлів із ненадійних сайтів, оскільки висока ймовірність не тільки підхопити вірус, а й вивантажити свій профіль.
- Не натискайте на посилання в підозрілих листах. Хакерам не потрібно багато робити, щоб взламати Вас, лише щоб Ви зробили декілька простих і звичних для Вас кроків.
- Не розповсюджуйте надто багато особистої інформації в соціальних мережах.
- Прогляньте й налаштуйте приватність у своїх акаунтах у соціальних мережах.
- Блокуйте підозрілих друзів на Facebook, Telegram, Viber та інших соціальних мережах.
- Використовуйте двофакторну аутентифікацію по можливості.
- По можливості налаштовуйте не паролі, а ключові фрази. Ключові фрази - це свого роду варіант дуже довгого паролю: ви можете налаштувати питання "Яка моя улюблена пісня?" як ключову фразу. Відповідь на неї буде складатися із більшої кількості символів, ніж просто пароль. Такий тип захисту складніше обійти.
- Видаляйте старі дані, які Вам більше не потрібні та одразу записуйте поверх них нову інформацію, аби видалені файли було неможливо відновити за допомогою спеціального програмного забезпечення.

ЯКІ МАТЕРІАЛИ МОЖУТЬ ДОПОМОГТИ НАВЧИТИ ДІТЕЙ ПРАВИЛ КІБЕРБЕЗПЕКИ

У пригоді стануть:

- **Блог “*Хакер, що біжить*“**, який веде експерт із кібербезпеки **Володимир Стиран**. Він ділиться досвідом і дає корисні поради. Наприклад, він описує загальні та детальні правила, як не стати кібержертвою. Ідеться про підозрілі посилання та пристрої, як вигадати надійний пароль, чому його варто тримати в секреті, навіщо потрібна двофакторна автентифікація, які месенджери безпечні, як працює шифрування даних, чому потрібно встановити антивірус, навіщо робити резервні копії, що таке мобільна безпека та як із нею бути тощо.

- **Онлайн-курс “Основи кібербезпеки для школярів”**, створений CRDF Global в Україні у співпраці з ГО “Смарт Освіта” та Technomatix. Він повністю безплатний та скоро буде у відкритому доступі. Слідкуйте за оновленнями на сайті “Нова українська школа”. Цей курс допоможе відрізнити правду від фейків, розкаже, з ким спілкуватися в інтернеті безпечно, а хто – насправді кіберзлочинець.

А ще під час проходження курсу діти дізнаються про те, як захистити гаджет, як шукати безпечні відео та інформацію в інтернеті, якою інформацією можна ділитися, про SMS-шахрайство, цифрові сліди, онлайн-ігри та офлайн-проблеми, безпеку комп’ютера, фейки і як їх розпізнати, як захистити інформацію, про що розповідають акаунти, більше про соціальні мережі, загрози інформаційного простору, соціальну інженерію, заробіток в інтернеті, онлайн-ігри, основні помилки користувачів та можливі наслідки, типи шкідливих програм, основні правила захисту інформації, що робити, якщо кіберзлочин усе-таки стався, та багато іншого.

Уся інформація подається через цікаві слайд-шоу, відео, інтерактиви, вправи та практичні завдання, максимально наближені до реальних ситуацій. Курс поділений на групи: для дітей 1–4, 5–6, 7–9 і 10–11 класів. Наприкінці учасники отримають сертифікати, що засвідчить їхні знання з кібербезпеки. (джерело: https://nus.org.ua/articles/shho-take-kiberbezpeka-yak-vchyty-ditej-buty-obachnymy-v-interneti-ta-korysni-resursy-dlya-navchannya/).

Директор НЕНЦ Володимир ВЕРБИЦЬКИЙ