**7 лютого 2017 року** у навчальних закладах міста Дніпра пройшли заходи, присвячені Всесвітньому дню безпечного Інтернету.

Одним із таких заходів став всеукраїнський вебінар в системі Cisco Webex під егідою програми Мережних академій Cisco та компанії ERC.

Захід відбувся за підтримки Центру підготовки інструкторів Cisco Національного гірничого університету (керівник – професор Цвіркун Л.І.), управління освіти департаменту гуманітарної політики Дніпровської міської ради (начальник – Марусов О.В.), адміністрації Дніпропетровського коледжу ракетно-космічного машинобудування ДНУ ім. Олеся Гончара (директор – Романовський О. М.). До участі у вебінарі долучились учні загальноосвітніх навчальних закладів міста №№ 23, 34, 37, 46, 53, 61, 62, 79, 89, 120, 137.

На вебінарі фахівці з кібербезпеки виступили з повідомленнями:

* «Захист даних в мережі шифруванням» (лектор: Полторак Вадим Петрович, НТУУ «КПІ ім. І.Сікорського», к.т.н., доцент кафедри автоматики і управління в технічних системах);
* «Гігієна в Інтернеті» (лектор: Вікторія Іцкович, ERC, директор дивізіону архітектурних рішень, керівник напрямку ІТ-безпеки)

та відповіли на запитання учнів.

Протягом години до експертів надійшло 50 запитань . Всі відповіді розміщено на сторінці курсу мережної академії Cisco «Вступ до кібербезпеки», до якого отримав доступ кожен учасник вебінару.

Учні також пройшли онлайн-тестування «Перевір на безпечність свою поведінку в Інтернет-просторі». За його результатами вони визначили ризики онлайн поведінки і отримали поради щодо того, як зробити свою поведінку в Інтернеті безпечнішою. Ось деякі з них:

* **Завжди оцінюйте, яку інформацією ви поширюєте в соціальних мережах, і з ким варто нею поділитися.**

Чим більше інформації Ви поширюєте в соціальних мережах, тим більше Ви дозволяєте зловмиснику дізнатися про Вас. Дізнавшись більше інформації про Вас, зловмисник отримує набагато більше можливостей для цілеспрямованої атаки. Наприклад, Ви повідомили всьому світу, що відвідали автоперегони. Зловмисник може надіслати Вам підроблений електронний лист від імені компанії, яка відповідає за продаж квитків на автоперегони. Цей лист буде виглядати дуже переконливо через те, що Ви дійсно тільки-но відвідали цю подію.

* **При створенні нового облікового запису для онлайнової служби створюйте абсолютно новий надійний пароль.**

Повторне використання паролів є поганою практикою, відмовтеся від неї. Якщо Ви повторно використовуєте пароль на сервісі, який вже знаходиться під контролем зловмисників, вони спробують від Вашого імені скористатися іншими сервісами і ці спроби матимуть успіх. А Ви матимете проблеми.

* **Не натискайте вбудовані посилання, отримані електронною поштою.**

Електронні листи можуть бути легко підроблені і при цьому виглядати як справжні. Підроблені електронні листи часто містять посилання на шкідливі сайти або шкідливі програми.

* **Не погоджуйтеся на встановлення будь-якого небажаного програмного забезпечення, особливо якщо ця пропозиція надходить з веб-сторінки.**

Наприклад, під час відвідування сайту відображається спливаюче вікно. У ньому зазначається, що Ваш комп'ютер знаходиться під загрозою і Ви повинні завантажити та встановити програму діагностики для його захисту. Вкрай малоймовірно, що веб-сторінка пропонує Вам справжнє оновлення програмного забезпечення. Закрийте браузер, ні в якому разі не натискаючи на спливаюче вікно, і використайте для перевірки оновлень інструменти операційної системи.

* **Завантажуйте програми тільки з офіційних сайтів компаній або фізичних осіб.**

Якщо Ви дізналися про цікаву для Вас програму і вирішили спробувати її використовувати, увімкніть розум, перш ніж дозволити запустити програму. Переконайтеся, що компанія або фізична особа, яка пропонує програму, є її законним автором. Не встановлюйте програму з підозрілого ресурсу.

* **Якщо Ви знайшли USB-носій невідомого походження, ні в якому разі не беріть його.**

USB-носії і флеш-накопичувачі містять крихітний контролер, який дозволяє комп'ютерам зв'язуватися з ними. Цей контролер можна інфікувати і після підключення носія до комп'ютера почнеться встановлення шкідливих програм на цей комп'ютер. Оскільки шкідливе програмне забезпечення міститься в самому USB контролері, а не в області даних, ніякі дії з очищення носія або перевірки антивірусним ПЗ не дозволяють виявити та видалити шкідливе програмне забезпечення.

* **Не використовуйте невідомі Wi-Fi точки доступу.**

Намагайтеся знайти довірене з'єднання. Зловмисники часто розгортають фальшиві точки доступу Wi-Fi, щоб заманити користувачів. Оскільки зловмисник має доступ до всієї інформації, яка проходить через таку фальшиву точку доступу, то підключені до неї користувачі дуже ризикують. На крайній випадок використовуйте такі точки доступу тільки з шифруванням трафіку через VPN. Ніколи не надавайте конфіденційні дані, такі, як номери кредитних карток, коли користуєтесь невідомою мережею (дротовою або бездротовою).

Більше корисних порад щодо безпеки в Інтернеті читайте на сторінці ***Психологічна служба*** у розділі ***Методична робота*** нашого сайту.