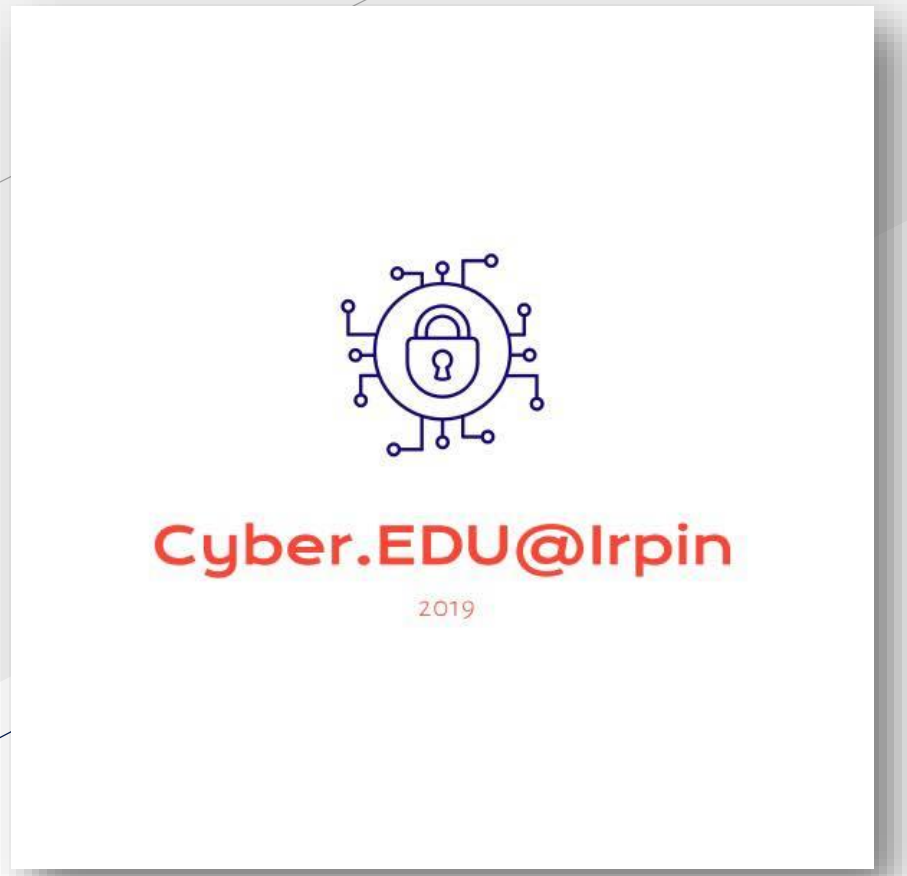
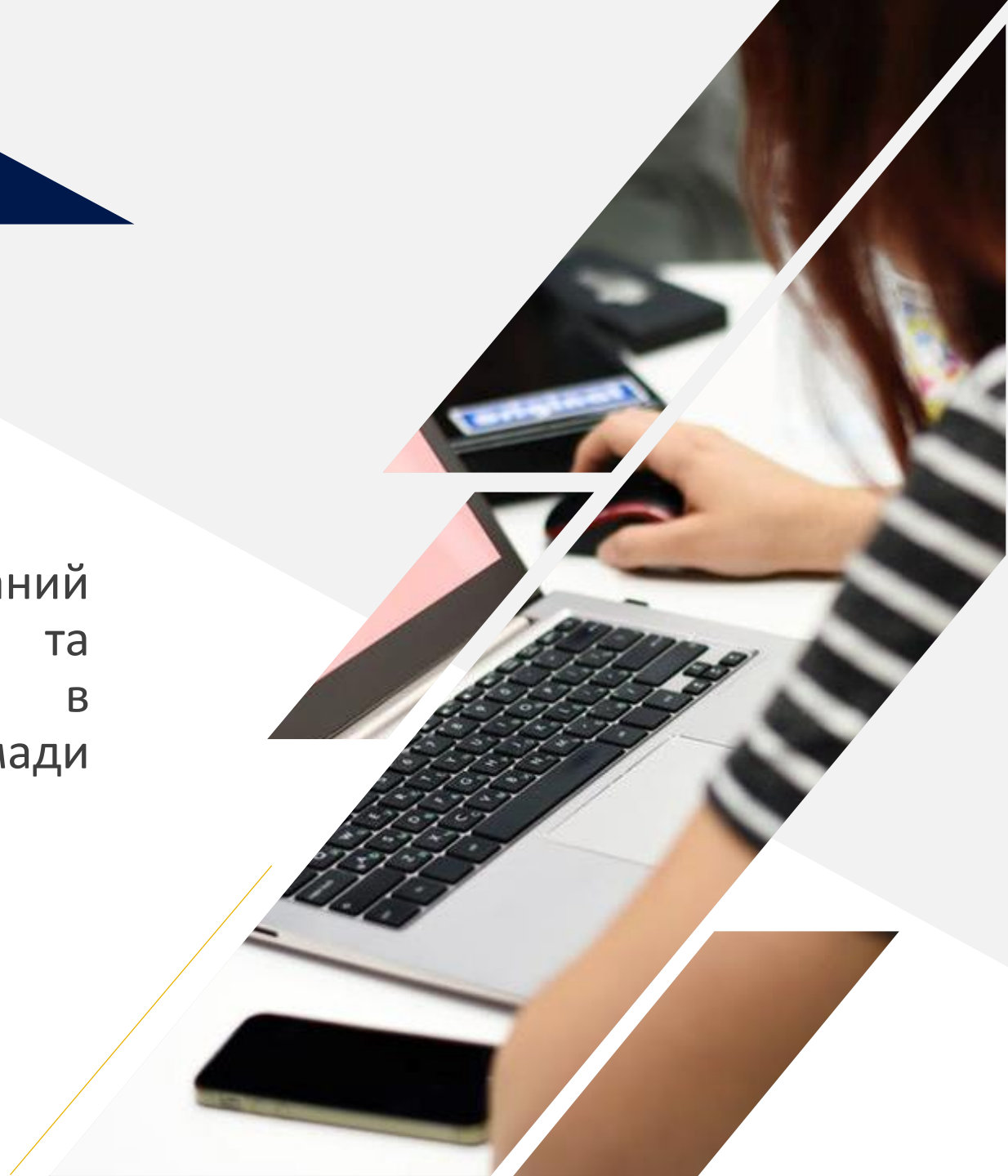


Cyber.EDU@Irpin

Cybersecurity: proactive community

Cyber.EDU@Irpin

- це освітньо-культурний проект, спрямований на підвищення цифрової грамотності та культури безпекового поводження в кіберпросторі серед населення громади м. Ірпеня



Марта Яцишин (УАКІБ, ІАР), +38 093 772 12 07,
martayatsyshyn@gmail.com

Cyber.EDU@Irpin

2019

Irpin Development Agency

IMP

Управління освіти і науки
Ірпінської міської ради Київської області

ІМГР
ІРПІНСЬКА МОЛОДІЖНА ГРОМАДСЬКА РАДА

cisco
Networking Academy

Irpin Development Agency

https://www.facebook.com/irpinagency/

Ірпінська агенція розвитку (IAP)
Irpin Development Agency

Незалежне недержавне неприбуткове громадське об'єднання, створене з метою консолідації зусиль усіх її членів для підтримки місцевих ініціатив та практичному втіленню необхідних для міста проектів структурної перебудови на локальному, регіональному, національному та міжнародному рівнях. Агенція здійснює залучення інвестицій в економіку міста, розвиток підприємництва, підготовку та реалізацію проектів у соціальній та гуманітарній сферах, бере участь у реалізації Стратегії розвитку міста.

Марта Яцишин (УАКІБ, IAP), +38 093 772 12 07,
martayatsyshyn@gmail.com

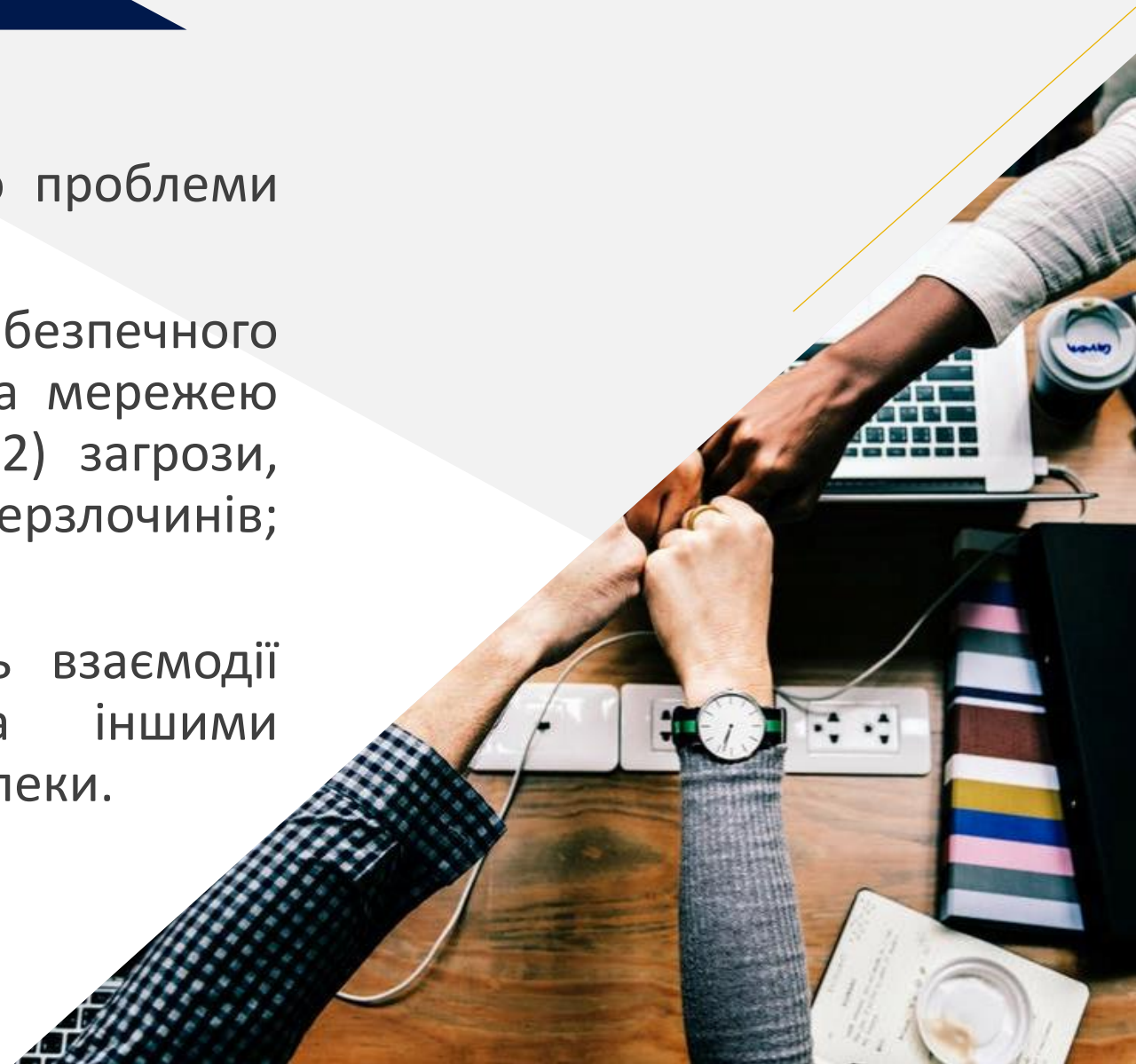
https://uacs.kiev.ua/

Українська академія кібербезпеки (УАКІБ)
Ukrainian Academy of Cyber Security

Громадська організація, метою діяльності якої є вивчення, узагальнення і розповсюдження національних і міжнародних наукових, освітніх і науково-технічних досягнень у сфері кібербезпеки, захисту інформації в інформаційно-телекомунікаційних системах, безпечного використання інформаційних технологій і систем, сприяння найбільш повному використанню цих досягнень в інтересах забезпечення інформаційної безпеки України та її соціально-економічного розвитку, сприяння розвитку і відтворенню інтелектуального потенціалу українського суспільства.

Завдання проекту:

- привернути увагу населення регіону до проблеми кібербезпеки;
- поширити інформацію про: 1) правила безпечного користування комп’ютерною технікою та мережею Інтернет, а також основи кібергігієни; 2) загрози, види способи здійснення і наслідки кіберзлочинів; методи і способи захисту.
- розповсюдити інформацію про модель взаємодії населення з правоохоронними та іншими державними органами з питань кібербезпеки.



Марта Яцишин (УАКІБ, ІАР), +38 093 772 12 07,
martayatsyshyn@gmail.com

Цільова аудиторія:

- учні загальноосвітніх шкіл регіону (8-10 класи);
- батьки учнів загальноосвітніх шкіл регіону;
- вчителі та інші працівники загальноосвітніх шкіл регіону;
- представники громадських організацій;
- агентства регіонального розвитку;
- активна молодь;
- місцеві ЗМІ.

Марта Яцишин (УАКІБ, ІАР), +38 093 772 12 07,
martayatsyshyn@gmail.com

Ірпінська спеціалізована загальноосвітня школа І-ІІІ ст. художнього профілю №1 м. Ірпінь	Ірпінська загальноосвітня школа І-ІІІ ст. №18 смт. Коцюбинське
Ірпінська спеціалізована загальноосвітня школа І-ІІІ ст. з поглибленим вивченням економіки та права №2 м. Ірпінь	Ірпінський навчально-виховний комплекс «Школа І-ІІ ст. – Коцюбинський гуманітарний ліцей» смт. Коцюбинське
Ірпінська спеціалізована загальноосвітня школа І-ІІІ ст. №12 з вивченням іноземних мов м. Ірпінь	Ірпінське навчально-виховне об’єднання «Освіта» м. Ірпінь
Ірпінська загальноосвітня школа І-ІІІ ст. №17 м. Ірпінь	Ірпінське навчально-виховне об’єднання «Ірпінський ліцей інноваційних технологій – Мала академія наук» м. Ірпінь

Ірпінська загальноосвітня школа І-ІІІ ст. №3
м. Ірпінь

Ірпінська загальноосвітня школа І ступеня №11
смт. Ворзель

Ірпінський академічний ліцей
м. Ірпінь

Ірпінська загальноосвітня школа І-ІІІ ст. №3
смт. Ворзель

Ірпінська загальноосвітня школа І-ІІІ ст. №13
смт. Гостомель

Ірпінська загальноосвітня школа І-ІІІ ст. №14
смт. Гостомель

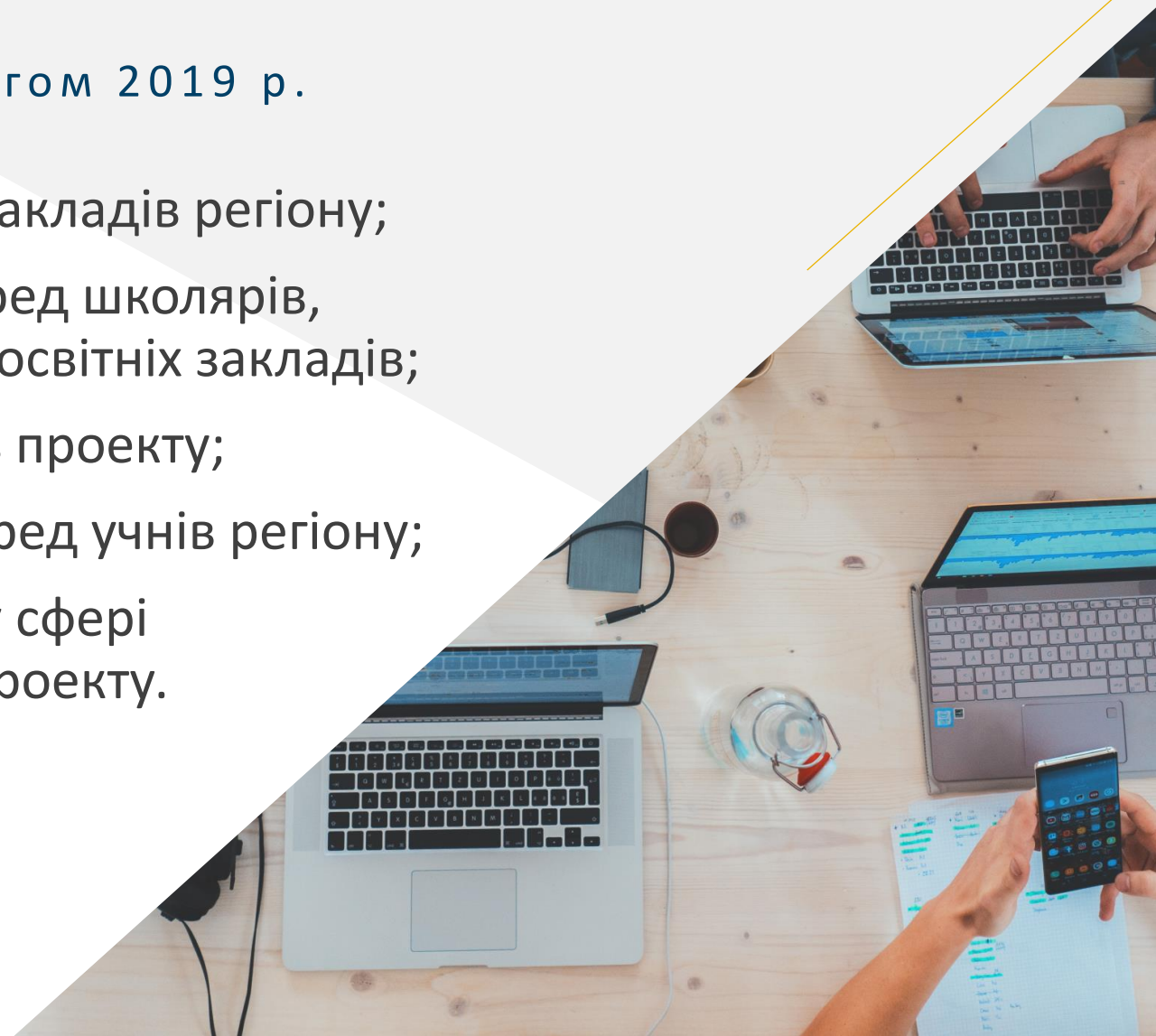
Проект охоплює 14 освітніх закладів

Марта Яцишин (УАКІБ, ІАР), +38 093 772 12 07,
martayatsyshyn@gmail.com

Етапи проекту

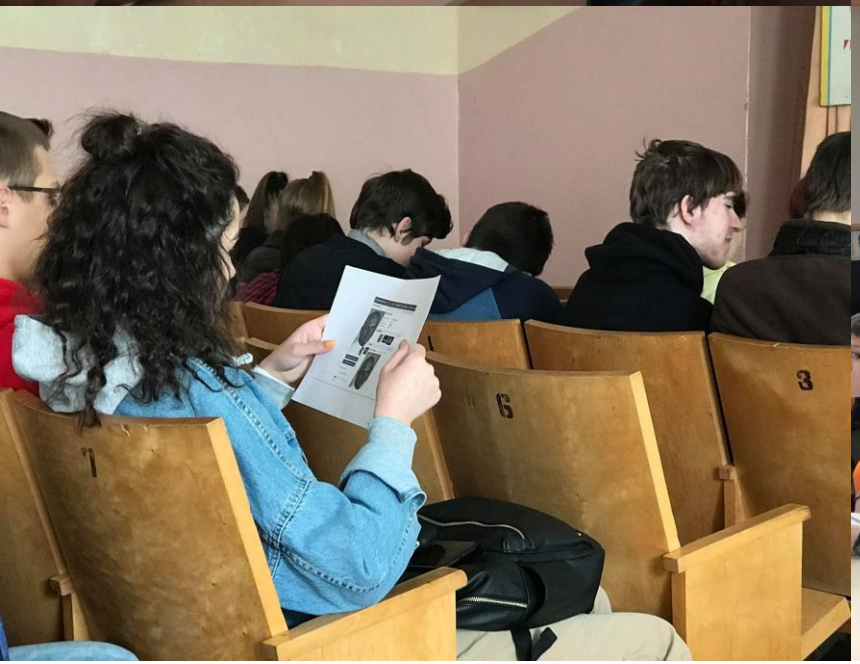
Реалізація проекту здійснюється протягом 2019 р.

1. Практичні тренінги для учнів освітніх закладів регіону;
2. Поширення друкованих матеріалів серед школярів, батьків, вчителів та інших працівників освітніх закладів;
3. Опитування різних категорій учасників проекту;
4. Проведення конкурсу відеороликів серед учнів регіону;
5. Заключний форум за участі експертів у сфері кібербезпеки і підведення підсумків проекту.



Марта Яцишин (УАКІБ, ІАР), +38 093 772 12 07,
martayatsyshyn@gmail.com



Марта Яцишин (УАКІБ, ІАР), +38 093 772 12 07,
martayatsyshyn@gmail.com

CYBER.EDU@IRPIN

ПАМ'ЯТКА ПРО БЕЗПЕЧНЕ ПОВОДЖЕННЯ У КІБЕРПРОСТОРІ

Irpin Development Agency

ІМГР

1. БЕРЕЖИ СВОЇ ПЕРСОНАЛЬНІ ДАНІ

Завжди вказуй лише мінімум необхідної інформації про себе, батьків та інших людей. Не треба розповсюджувати без необхідності прізвище та ім'я, адресу дому чи школи, вік, медичні, фінансові чи інші особисті дані, номери телефонів. Не поширюй багато інформації про себе у соціальних мережах

2. НЕ ЗАБУВАЙ, ТВОЇ ДАНІ МОЖУТЬ БУТИ ВИКРАДЕНІ

Завжди пам'ятай про те, що вся твоя інформація, фотографії, листування чи переписки у будь-який час можуть опинитися в руках зловмисника. А тому не зберігай і не поширюй нічого, що може тобі нашкодити

3. ЗАХИЩАЙ СВОЇ ПРИСТРОЇ

Слідкуй щоб на пристроях, якими ти користуєшся, були включені антивірусні та інші захисні програми

4. ПАМ'ЯТАЙ ПРО СИМПТОМИ ШКІДЛИВИХ ПРОГРАМ

Знижується швидкодія комп'ютера. Комп'ютер часто зависає або дає збої. Знижується швидкість перегляду веб-сторінок. З'являються незрозумілі проблеми з мережними з'єднаннями. Файли змінюються або видаляються. З'являються невідомі файли, програми чи значки на робочому столі. Електронна пошта надсилається без відома

5. ВСТАНОВЛЮЙ НАДІЙНІ ПАРОЛІ

Щоб пароль був надійним: не використовуй слова із словника або імена будь-якою мовою; не використовуй імена комп'ютерів або імена облікових записів; якщо це можливо, використовуй спеціальні символи, такі як ! @ # $ % ^ & * (. Довжина пароля має бути 10 та більше символів. Найкращим паролем буде ціла фраза з використанням спеціальних символів, яку зрозумієш тільки ти.
Нікому крім батьків не давай свої паролі

6. НЕ КОРИСТУЙСЯ ОДНИМ ПАРОЛЕМ

Для кожного пристрою та Інтернет-ресурсу створюй новий унікальний пароль. Якщо не можеш запам'ятати всі паролі, використовуй менеджери паролів, які зберігають та шифрують їх. Кожних три місяці рекомендовано змінювати паролі.Нікому крім батьків не давай свої паролі

7. ОБАЧНО ВИКОРИСТОВУЙ ВІДКРИТІ ПУБЛІЧНІ МЕРЕЖІ WI-FI

Пам'ятай, що використання публічних мереж Wi-Fi є небезпечним. Підключайся до них лише за особливої необхідності. Не надсилай за допомогою такого підключення важливі документи та інформацію. Забороняй спільне використання файлів, а також бажано включай програми шифрування (VPN)

8. ЗАХИЩАЙ СВОЮ РОБОТУ В ІНТЕРНЕТІ

Користуючись Інтернетом включай приватний (анонімний) режим у веб-браузері. За можливості на сайтах вибирай двофакторну автентифікацію. Прочитай та налаштуй приватність у соцмережах. Блокуй підозрілі сторінки у соцмережах. Не переходь на шкідливі сайти та за ненадійними посиланнями

9. БУДЬ УВАЖНИМ ДО ЕЛЕКТРОННИХ ЛИСТІВ

Завжди звертай увагу на електронну пошту відправника, вона має відповідати отриманому листу і не містити помилок чи символів. Не переходь автоматично за надісланими посиланнями, не відкривай надіслані файли. Будь особливо уважним, якщо отримав листа від людини чи організації, яких не знаєш особисто. Ніколи не відповідай на підозрілі листи, навіть якщо вони образливі чи грубі

10. НЕ ДОВІРЯЙ НЕЗНАЙОМЦЯМ

Незнайомець в Інтернеті може виявитись не тим, за кого себе видає. Не довіряй одразу незнайомій людині, не розповідай про себе чи рідних. Не надсилай особистих фотографій. Не погоджуйся на зустріч. А також будь обачним і не виконуй прохань незнайомців

11. ЗАВЖДИ ЗВЕРТАЙСЯ ДО БАТЬКІВ ЧИ ІНШИХ ДОРОСЛИХ

Якщо відбувається щось незвичайне: дивно працює твій пристрій, отримав підозрілого листа, новий Інтернет-знайомий дивно поводиться, потрібно здійснити оплату через Інтернет – звертайся до батьків чи інших дорослих.

12. ЗЛОЧИНИ У КІБЕРПРОСТОРІ – ТЕЖ ЗЛОЧИНИ

Не погоджуйся здійснювати неправомірні дії в Інтернеті. За це передбачено кримінальну відповідальність.

ПАМ'ЯТКА ДЛЯ БАТЬКІВ ПРО БЕЗПЕЧНЕ ПОВОДЖЕННЯ У КІБЕРПРОСТОРІ

CYBER.EDU@IRPIN

Irpin Development Agency

ІМГР

1. ВСТАНОВІТЬ ВЛАСНІ ПРАВИЛА КОРИСТУВАННЯ КОМП'ЮТЕРНОЮ ТЕХНІКОЮ ТА ІНТЕРНЕТОМ

Визначте скільки часу дитина може проводити за комп'ютером (ноутбуком, планшетом, мобільним телефоном), на які ресурси заходити, якими програмами користуватися. Обов'язково дотримуйтесь встановлених правил

2. ПЕРЕКОНАЙТЕСЬ, ЩО ПРИСТРІЙ ЯКИМ КОРИСТУЄТЬСЯ ДИТИНА ЗАХИЩЕНИЙ

Встановіть та вчасно оновлюйте антивірусні та інші захисні програми. Переконайтесь, що вони працюють і періодично проводьте огляд пристроїв (кожних 3 місяці). Використовуйте надійні паролі. Обов'язково захищайте домашню мережу.

Симптоми шкідливих програм: знижується швидкодія комп'ютера; комп'ютер часто зависає або дає збої; знижується швидкість перегляду веб-сторінок; з'являються незрозумілі проблеми з мережними з'єднаннями; файли змінюються або видаляються; з'являються невідомі файли, програми чи значки на робочому столі; електронна пошта надсилається без відома та згоди.

3. ЗАХИСТІТЬ ІНФОРМАЦІЮ

Переконайтесь, що важливі файли не зберігаються на пристрої, яким користується дитина. Періодично здійснюйте резервне копіювання даних, зокрема на інші носії, а також в хмарних сервісах. Використовуйте шифрування важливих файлів.

4. КОРИСТУЙТЕСЯ ПРОГРАМАМИ, ЯКІ ФІЛЬТРУЮТЬ ОТРИМАННЯ ІНФОРМАЦІЇ

Встановіть програми веб фільтрації батьківського контролю. Це надасть змогу автоматично обмежити доступ дітей до шкідливих ресурсів в мережі Інтернет. Здійсніть налаштування веб фільтру, обравши необхідний рівень обмежень, типи забороненого вмісту, перелік небажаних сайтів та ін.

5. ЦІКАВТЕСЬ ЖИТТЯМ ДИТИНИ ОНЛАЙН

Розмовляйте з дитиною про її дії в мережі. Дізнавайтесь, які сайти вона любить відвідувати, з ким знайомиться і спілкується. Розпитуйте про ігри, в які вона грає. Заохочуйте дитину ділитись інформацією, отриманою в Інтернеті.

6. СЛІДКУЙТЕ ЗА ВИТРАТАМИ ДИТИНИ НА МОБІЛЬНИЙ ЗВ'ЯЗОК ТА ІНТЕРНЕТ

Оператори мобільного зв'язку надають сервіси, за допомогою яких можна переглядати витрати певного мобільного номеру.

7. БУДЬТЕ ДРУЗЯМИ У СОЦІАЛЬНИХ МЕРЕЖАХ

Зареєструйтесь у соціальних мережах, якими користується Ваша дитина. Спілкуйтесь там, звертайте увагу на інтереси дитини, її оточення і контент, який вона створює. Налаштуйте разом із дитиною приватність її сторінки. Допомагайте блокувати підозрілих користувачів

8. НАВЧІТЬ ДИТИНУ НЕ ПОШИРЮВАТИ ОСОБИСТУ ІНФОРМАЦІЮ ПРО СЕБЕ І СВОЮ РОДИНУ

Поясність, якою інформацію не потрібно ділитися і чому (прізвище та ім'я, адреса дому чи школи, вік, медичні, фінансові чи інші особисті дані, номери телефонів тощо). Домовтесь, щоб у випадках, коли необхідно вказати власні дані чи дані інших членів сім'ї, дитина спочатку обов'язково радилась з Вами

9. СЛІДКУЙТЕ ЗА ФІНАНСОВИМИ ОПЕРАЦІЯМИ ДІТЕЙ

Домовтесь, що всі фінансові операції у кіберпросторі діти здійснюють лише за Вашого відома і користуючись захищеним з'єднанням. Не дозволяйте використовувати Ваші банківські карти самостійно. Перевіряйте ресурси, на яких потрібно здійснити оплату

10. НАВЧІТЬ ДИТИНУ ВІДПОВІДАЛЬНОМУ ПОВОДЖЕННЮ В КІБЕРПРОСТОРІ

Будь-яка протизаконна діяльність в Інтернеті є карною, а тому діти повинні усвідомлювати значення своїх дій.

11. ПІДТРИМАЙТЕ ДИТИНУ, ЯКЩО ВОНА СТАЛА ЖЕРТВОЮ

У випадку кібербулінгу чи сексингу, а також інших посягань, не панікуйте. Підтримайте Вашу дитину. Звертайтесь до технічної підтримки ресурсів з метою видалення шкідливого контенту. Не беріть участь в обговоренні, не відповідайте на коментарі. Якщо дитина стала жертвою кіберзлочину обов'язкового звертайтесь до органів Національної поліції України, зокрема Департаменту кіберполіції

При розробці тренінгової частини, а також друкованих матеріалів проекту використовувались матеріали надані:

1) Українською академією кібербезпеки;
2) Cisco Networking Academy, зокрема курс «Вступ до кібербезпеки»;
3) Навчальний посібник із цифрового громадянства й безпеки, розроблений Google у співробітництві з Альянсом із захисту безпеки користувачів в Інтернеті (Internet Keep Safe Coalition, iKeepSafe.org)

Очікувані результати:

1. Населення регіону отримає базові знання з питань кібербезпеки;

2. Підвищення рівня свідомого поводження населення регіону в кіберпросторі;

3. Підвищення безпечності і захисту комп’ютерних систем і мереж, які перебувають у домашньому користуванні, а також школах регіону;

4. Підвищення контролю і відповідального ставлення батьків та вчителів до кібербезпеки дітей;

5. Діти отримають правильне сприйняття моделей поведінки у кіберпросторі, в тому числі засудження злочинних дій, що зменшить їх залучення до кіберзлочинної діяльності

Марта Яцишин (УАКІБ, ІАР), +38 093 772 12 07,
martayatsyshyn@gmail.com

Cyber.EDU@Irpin

2019

Дякую за увагу!

Марта Яцишин

+38 093 772 12 07

martayatsyshyn@gmail.com