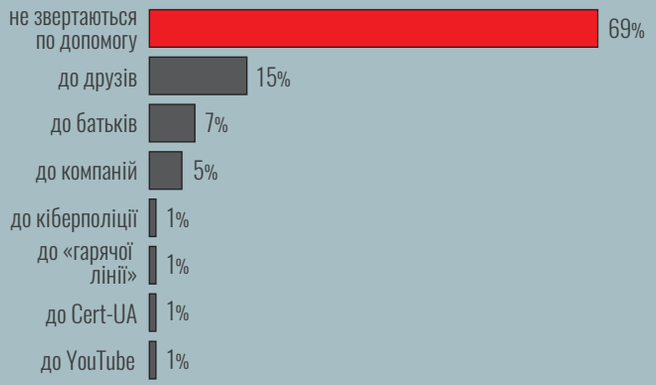
1 МОЛОДЬ НЕ ЗНАЄ, ДО КОГО ЗВЕРТАТИСЬ ПО ДОПОМОГУ В РАЗІ ЗУСТРІЧІ З КІБЕРЗАГРОЗОЮ

На сьогодні у держави не існує власної «гарячої лінії» з питань кібербезпеки, зокрема окремої «дитячої» лінії. Така служба — Національна дитяча «гаряча лінія» — є лише в ГО «Ла Страда — Україна». Проте працює вона тільки чотири години на добу через нестачу коштів, і поки що не має ніякої підтримки з боку держави.

Діаграма №1. До кого звертаються підлітки по допомогу в разі зустрічі з кіберзагрозою



що робити?

- Поінформувати підлітків про існування Національної дитячої «гарячої лінії» — 0 800 500 335 або 116 123 (короткий номер з мобільного) — спільними зусиллями МОН, правоохоронних органів, навчальних закладів, операторів та провайдерів, IT бізнесу, медіа, громадських організацій
- Звернутись до міжнародних донорів та бізнесу за наданням фінансової підтримки Національної дитячої «гарячої лінії» та приєднання України до міжнародної мережі «гарячих ліній» InSafe. Закласти в державний бюджет статтю витрат на фінансування заходів з кібербезпеки для підлітків
- Розробити механізми взаємодії Національної дитячої «гарячої лінії» з українськими правоохоронними органами — спільними зусиллями громадськості, держави, бізнесу
- Забезпечити підтримку з боку CERT-UA (за підтримки приватного бізнесу та громадськості) механізмів та стандартів захисту і нформаційних ресурсів МОН та його підрозділів, навчальних та дитячих закладів

2 І МОЛОДІ, І ФАХІВЦЯМ БРАКУЄ ІНФОРМАЦІЇ ПРО ВИДИ КІБЕРЗАГРОЗ

Наприклад, не знаючи про те, як діють фішінгові сайти, молода людина несвідомо повідомляє злочинцям інформацію про себе, родичів та друзів. Цю інформацію шахраї використовують для оформлення кредиту, підробки документів, крадіжки коштів.

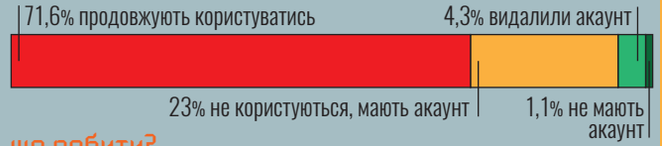
що робити?

- Розробити модель ризиків та алгоритм протидії кіберзагрозам для молоді — спільними зусиллями експертів правоохоронних органів, бізнесу, громадськості, молоді
- Проводити регулярні опитування молоді з питань кібербезпеки з врахуванням віку, освіти, засобів доступу до Інтернету, використовуючи ресурси фахівців МОН, соціологів, кіберполіції, бізнесу, громадськості, молоді. Широко презентувати та аналізувати результати досліджень
- Привести українську термінологію з кібербезпеки у відповідність до європейської

3 МОЛОДЬ НЕ УСВІДОМЛЮЄ РИЗИКИ ВІД КОРИСТУВАННЯ РОСІЙСЬКИМИ СОЦІАЛЬНИМИ МЕРЕЖАМИ І РОСІЙСЬКИМ ТА/АБО ПІРАТСЬКИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ (ЗОКРЕМА, АНТИВІРУСАМИ)

Через російські соціальні мережі спецслужби отримують інформацію як про користувача, так і про його родичів, друзів, що може бути використано з підступною метою. Крім того, завдяки геотегам, користування цими сервісами дає змогу з'ясувати місцеперебування молодої людини.

Діаграма №2. Користування російськими соціальними мережами українськими підлітками



що робити?

- Розробити інформаційну кампанію про ризики користування російськими соціальними мережами і піратським та/або російським програмним забезпеченням — за участі соціологів, експертів з кібербезпеки, освітян, медійників, фахівців з PR і SMM та молоді
- Запровадити обов'язкову стандартизацію програмного забезпечення в навчальних закладах з метою неприпустимості використання піратського та/або російського програмного забезпечення, пропагувати відкрите програмне забезпечення — зусиллями МОН та правоохоронних органів, за участі приватних та громадських експертів
- Пропагувати українські інформаційні продукти, антивіруси — зусиллями медіа, активістів соціальних мереж, громадських організацій

4 МОЛОДЬ НЕ ЗНАЄ, ДЕ ШУКАТИ ІНФОРМАЦІЮ ПРО КІБЕРЗАГРОЗИ ТА ЯК УБЕЗПЕЧИТИСЯ ВІД НИХ

Зокрема, більше половини опитуваних визнають, що їм необхідно більше знань в сфері кібербезпеки. 62% з них не знають, де їх з найти. Найбільш поширеним джерелом інформації з питань кібербезпеки є соціальні мережі.

що робити?

- Розробити державну просвітницьку програму з кібербезпеки, орієнтовану на молодь (як в якості частини шкільного курсу з інформатики, так і в якості окремих курсів) — за участі міжнародних експертів, спільними зусиллями фахівців з державного, приватного та громадського секторів, обов'язково за участі молоді
- Розробити державну програму профілактичних заходів з кібербезки для навчальних закладів — за участі міжнародних експертів, спільними зусиллями фахівців з державного, приватного та громадського секторів, обов'язково за участі молоді
- Розробити стратегію просування інформації з питань кібербезпеки, про діяльність правоохоронних органів та про профілактичні заходи з кібербезпеки в соціальних мережах — спільними зусиллями фахівців з державного, приватного та громадського секторів, обов'язково за участі молоді
- Регулярно інформувати молодь про нові кіберзагрози та про те, як можна убезпечитись від них — зусиллями CERT-UA та кіберполіції за допомогою приватних та громадських фахівців, медіа, активістів соціальних мереж
- Просувати вже існуючі та створити нові он-лайн ресурси, що сприяють підвищенню рівня кібербезпеки молоді

5 СУСПІЛЬСТВУ БРАКУЄ УСВІДОМЛЕННЯ РИЗИКІВ, ДО ЯКИХ ПРИЗВОДИТЬ ВИКОРИСТАННЯ ПРОТИ МОЛОДІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, МАНІПУЛЮВАННЯ ДУМКАМИ ЗА ДОПОМОГОЮ СОЦІАЛЬНИХ МЕРЕЖ

За допомогою даних, які збираються про користувачів соціальних мереж, інформація подається таким чином, аби сформулювати певні «необхідні» замовнику погляди молоді.

що робити?

- Підтримати розроблені та сприяти розробці нових програм з розвитку критичного мислення, медіаграмотності та інформаційної гігієни, ввести їх в шкільну програму — зусиллями МОН та громадських організацій
- Провести інформаційну кампанію для усвідомлення молоддю ризиків поширення інформації про себе, своїх родичів та друзів в соціальних мережах — зусиллями офісу Омбудсмена, правоохоронних органів, МОН, соціологів, громадських організацій

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ

для Парламенту

Розробити та ухвалити Закон про кібербезпеку, який забезпечить створення ефективної системи кібербезпеки, в тому числі і молоді, та приведе українську термінологію в сфері кібербезпеки у відповідність до європейської

для Уряду і МОН

- Розробити комплексну державну програму просвітницьких та профілактичних заходів з кібербезпеки в навчальних закладах. Залучити до розробки програми експертів з кібербезпеки, представників бізнесу, громадськості, молоді
- Запровадити регулярне опитування молоді з питань кібербезпеки
- Проводити змагання «білих хакерів», олімпіади з питань кібербезпеки

для правоохоронних органів

- Налагодити співпрацю з Національною дитячою «гарячою лінією»
- Розробити стратегію інформаційної кампанії, метою якої є:

  - широке інформування про те, куди звертатися молоді в разі зіткнення з кіберзагрозами

  - своєчасне інформування про нові кіберзагрози та про те, як можна убезпечитись від них

  - широке інформування про результати розслідування інцидентів, особливо тих, де постраждалою стороною є молодь

  - активне використання соціальних мереж

для представників бізнесу

В рамках корпоративної соціальної відповідальності:

- долучитися до розробки інформаційної кампанії Уряду та МОН
- долучитися до проведення просвітницької роботи в сфері кібербезпеки в навчальних закладах
- долучитися до розробки онлайн-курсів та онлайн ресурсів з кібербезпеки для школярів та їх батьків, студентів

для шкіл

Проведення факультативних позакласних навчань для учнів за участю експертів з кібербезпеки (або демонстрація відеозаписів лекцій експертів — як українських, так і міжнародних)

для громадських організацій

- Брати участь в розробці інформаційної кампанії Уряду та МОН та ініціювати власні просвітницько-інформаційні кампанії
- Долучитися до проведення просвітницької роботи в сфері кібербезпеки в навчальних закладах
- Пропагувати українські інформаційні продукти, зокрема антивіруси

для молоді

- Брати активну участь в розробці та обговоренні законодавчих ініціатив та державних програм в сфері кібербезпеки
- Піклуватись про підвищення власного рівня обізнаності з питань кібербезпеки, медіаграмотності, інформаційної гігієни, свідомо ставитись до розповсюдження інформації про себе, своїх родичів та друзів
- Брати активну участь в підготовці та проведенні Українського Молодіжного Форуму з управління Інтернетом

ПРО ДОСЛІДЖЕННЯ

Дослідження проведене міжнародною громадською організацією «Європейська Медіа Платформа» за підтримки Counterpart International.

Дослідження складалось з двох частин;

анонімне опитування української молоді в трьох фокус-групах (кілька класів однієї з київських шкіл, один курс одного з київських коледжей, одна група одного з київських ВНЗ).
Загальна кількість респондентів — 95;

ознайомлення українських експертів з кібербезпеки з результатами опитування та прохання до них прокоментувати ці результати і відповісти на конкретні питання.
Загальна кількість опитаних експертів — 25.
Серед них — представники кіберполіції, CERT-UA, РНБОУ, приватного бізнесу, громадських організацій, незалежні експерти.

З результатами дослідження можна ознайомитись на сайті eump.org

Автор дослідження — Оксана Приходько
директор НУО «Європейська Медіа Платформа»
sana@eump.org

Сторінка на Facebook European Media Platform

USAID FROM THE AMERICAN PEOPLE

COUNTERPART INTERNATIONAL

Дослідження міжнародної громадської організації «Європейська Медіа Платформа»

КІБЕРБЕЗПЕКА ОЧИМА УКРАЇНСЬКОЇ МОЛОДІ