КОАЛІЦІЯ 1325 ЗАКАРПАТТЯ
ДОВІРА DÔVERA Товариство словацьких жінок
Kingdom of the Netherlands
UKRAINIAN WOMEN'S FUND

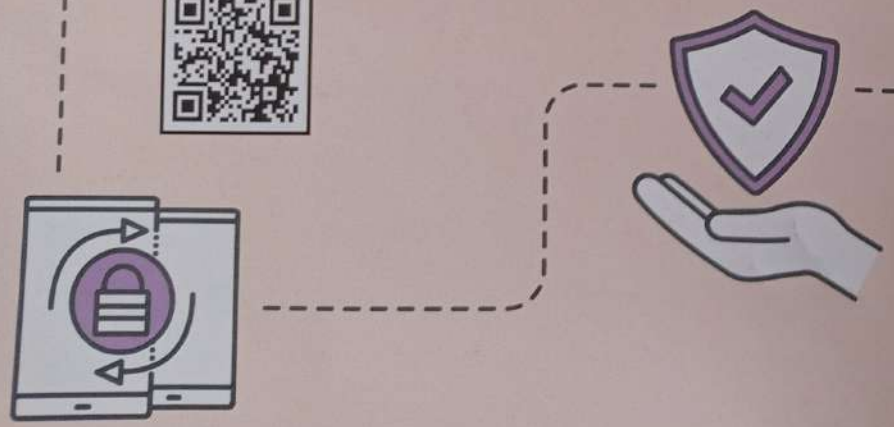
ДБАЙ ПРО СВОЮ БЕЗПЕКУ

Гаряча лінія для дітей - **116 111**

Урядова консультаційна лінія
з питань безпеки дітей в інтернеті - **1545**

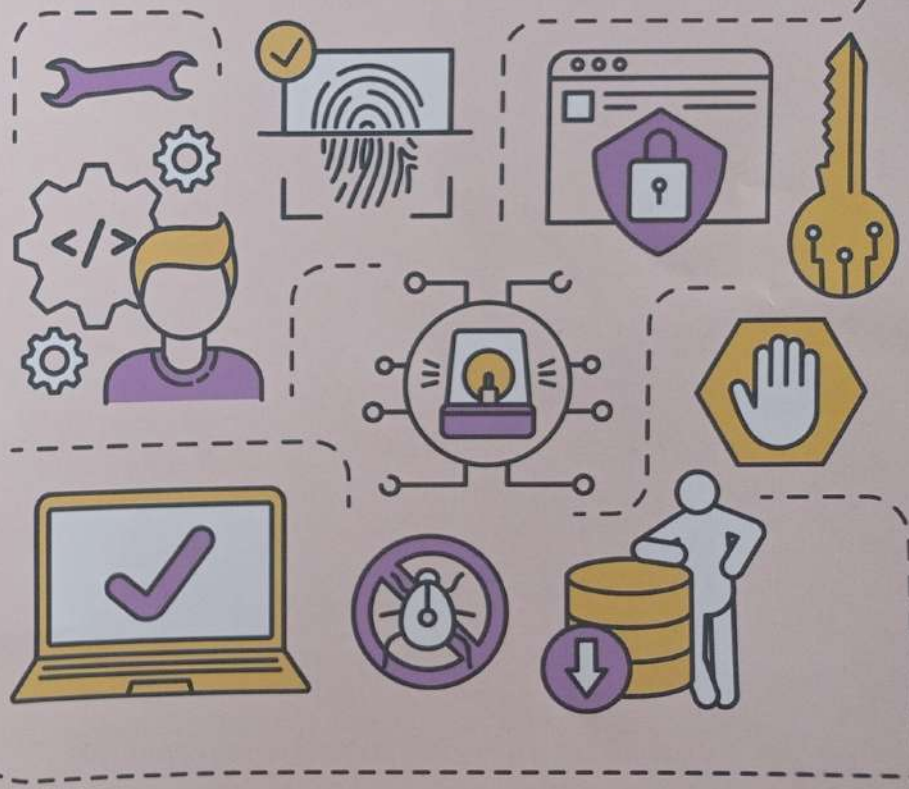
Національна дитяча гаряча лінія:
0-800-500-225

Посилання на звернення:
HTTPS://TICKET.CYBERPOLICE.GOV.UA/SEND



КОАЛІЦІЯ 1325 ЗАКАРПАТТЯ
ДОВІРА DÔVERA Товариство словацьких жінок
Kingdom of the Netherlands
UKRAINIAN WOMEN'S FUND

ЩО ВАЖЛИВО ЗНАТИ ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ



ІНФОРМАЦІЙНА БЕЗПЕКА
ЯК СЕБЕ ЗАХИСТИТИ

МІФИ ТА СТЕРЕОТИПИ

МІФ: *Інформаційна безпека - це проблема лише для великих компаній і урядів.*

ФАКТ: *Інформаційна безпека стосується кожного, хто користується Інтернетом. Зловмисники можуть атакувати будь-яку людину або організацію, яка має доступ до Інтернету.*

МІФ: *Якщо я не використовую Інтернет, мене не можуть зламати.*

ФАКТ: *Зловмисники можуть отримати доступ до вашої інформації, навіть якщо ви не користуєтеся Інтернетом. Вони можуть використовувати соціальну інженерію для отримання доступу до вашого комп'ютера або мобільного пристрою.*

МІФ: *Якщо я користуюся Wi-Fi, то моя безпека гарантована.*

ФАКТ: *Використання Wi-Fi може бути небезпечним, якщо ви не дотримуєтеся відповідних заходів безпеки. Зловмисники можуть отримати доступ до вашої інформації, якщо ви підключаєтесь до незахищеної Wi-Fi мережі.*

МІФ: *Якщо я використовую антивірус, я захищений від усіх загроз.*

ФАКТ: *Антивірус не може захистити вас від усіх видів загроз. Хоча він може захистити від деяких атак, але не від усіх. Крім того, він може бути неефективним, якщо не регулярно оновлювати його базу даних.*

МІФ: *Якщо у мене складний пароль, мої дані захищені.*

ФАКТ: *Зловмисники можуть використовувати різні методи, такі як соціальна інженерія, фішинг або шкідливе програмне забезпечення, щоб отримати доступ до вашого пароля.*

ЩО ВАЖЛИВО ЗНАТИ ПРО
ІНФОРМАЦІЙНУ БЕЗПЕКУ

ІНФОРМАЦІЙНА БЕЗПЕКА - *захищеність інформації та відповідної інфраструктури від випадкових або навмисних впливів, супроводжуються нанесенням шкоди власникам або користувачам інформації.*

Мета захисту інформації - *мінімізація втрат, викликаних порушенням цілісності або конфіденційності даних, а також їх недоступності для споживачів.*

Загрози інформаційній безпеці - *несанкціонований доступ до даних (наприклад, отримання сторонніми особами відомостей про стан рахунків клієнтів банку).*

Загрози цілісності - *несанкціонована модифікація, доповнення або знищення даних загрози доступності обмеження або блокування доступу до даних.*

СЕКСТОРШЕН - *це налагодження довірливих стосунків із дитиною в Інтернеті з метою отримання приватних матеріалів, шантажування та вимагання додаткових матеріалів або грошей.*

ФІШИНГ - *це спосіб обману в Інтернеті, коли зловмисники висилають електронні листи, текстові або голосові повідомлення від імені надійного джерела. Їх мета переконати людей відкрити доступ до особистої інформації або перейти за підозрілим посиланням.*

СТЕНОГРАФІЧНА АТАКА - *це техніка приховування інформації в інших формах даних, наприклад, коли у фотографіях зашифровують віруси, можна використовувати термін "вбудовані віруси" або "фото-віруси".*