

Діпфейк: що це таке та як його розпізнати?

Сьогодні більшість батьків переймаються безпекою дітей в онлайн-просторі. Попри свій вік, саме юні користувачі мережі потрапляють у групу ризику з викрадення особистих даних і втрати конфіденційності. За останні роки кількість онлайн-злочинів проти дітей зросла, що пов'язано з розвитком можливостей і технологій. Штучний інтелект, посідаючи почесне перше місце серед небезпек, допомагає злочинцям генерувати компроматні матеріали. Що таке діпфейк та як його розпізнати? Ця інструкція з кібербезпеки для дорослих і дітей.

Що таке діпфейк?

Існує такий термін, як «deepfake», що описує процес штучно (синтетично) створеного аудіо-, відео-, фотоматеріалу. Простими словами – це фейк, із допомогою якого можна скомпрометувати та підставити невинну особу. На початку свого існування ця історія розвивалася та сприймалася як цікавий розважальний контент. Можна було станцювати з Леонардо Ді Капріо на Титаніку чи врятувати світ із Месниками. Та із часом зловмисники почали використовувати діпфейки для шантажу та вимагання, створюючи неправдивий контент. Найвразливішими виявилися саме діти молодшого віку та підлітки, адже через свій вік вони довірливіші.

Як розпізнати діпфейк?

Технології завжди мають позитивний та негативний вплив. І якщо діпфейк може створити небезпеку в мережі, то існують інструменти для запобігання.

Для перевірки зображення можна використовувати такі ресурси:

FotoForensics, Al or Not, Fake news debunker by InVID & WeVerify.

Для розпізнавання аудіодіпфейків також існують сервіси, як от:

AI Voice Detector, Al or Not, PlayHT, Resemble Detect.

Ви можете використовувати будь-які інші джерела для перевірки інформації, зважаючи на їхню країну походження та перевіряючи репутацію ресурсу в інтернеті.

Як розпізнати дідфейк на фото?

- риси обличчя виглядають як лялькові;
- глянцевого колір шкіри;
- розмиті деталі;
- неприродний фон;
- неприродні пози;
- викривлені символи.

Як розпізнати дідфейк на відео?

- відео має погану якість;
- міміка спікера, особливо рухи губ, не повністю збігається зі сказаним;
- у відео немає сторонніх звуків та шумів;
- голос відрізняється від реального.

Як уникнути наслідків необачної поведінки в мережі?

У квітні 2024 року CRDF Global в Україні за підтримки Державного департаменту США спільно з РНБО та МОН України запустили всеукраїнську інформаційну кампанію щодо особистої кібербезпеки. Її мета – підвищити загальний рівень обізнаності про загрози, що існують, та навчити українців основ кібергігієни. Важливо, що автори кампанії регулярно аналізують ситуацію з кібербезпеки у світі та розробляють найактуальніші правила для того, щоб захистити себе та своїх рідних від наслідків кібератак і необачної поведінки в інтернеті.

Головні правила кібергігієни

• Надійний пароль – перша лінія оборони персональних даних

– **qwerty1234** – це приклад пароля, який не варто ставити на жоден акаунт.

– Захистіть ваші дані: придумайте складні паролі, зберігайте їх у менеджері паролів і не ігноруйте додатковий захист акаунту через вашу електронну пошту або номер мобільного (двофакторна аутентифікація).

• Переходьте лише за перевіреними посиланнями.

Листи з новинами про виграші найчастіше – неправда. Візьміть за звичку перевіряти в пошуковикі всі незрозумілі посилання навіть від надійних контактів, адже їхні акаунти теж можуть зламати. І не довіряйте повідомленням, які ваша електронна пошта чи соціальні мережі самотійно маркують як спам.

- **Безплатний WiFi – джерело легкого доступу до приватності користувача.**

- Відкритий WiFi по всьому місту – це зручно, адже можна залишатися на зв'язку будь-коли. Та користуватися таким інтернетом необхідно з обачністю.

- Перевіряйте WiFi, до якого підключаєтеся: відкритим мережам у кафе, ТРЦ чи інших публічних місцях не варто довіряти. Їх легко зламати або підробити, і всі важливі дані опиняться в руках у кіберзлочинців.

- Якщо потрібно переказати гроші, вказати паспортні дані, попрацювати з важливими документами чи виконати інші чутливі операції, використовуйте мобільний інтернет як точку доступу.

- **Антивірус – ваш особистий охоронець 24/7.**

- Це програма, що захищає ваш гаджет від вірусів. Вона працює у фоновому режимі й без упину перевіряє все, що відбувається на пристрої: аналізує всі активні програми, файли та сайти.

- **Фізичний захист гаджетів – ефективна відповідь зловмисникам.**

- Блокування екрана паролем – це найпростіший захист, що має бути на всіх ваших пристроях: ноутбучі, планшеті й смартфоні.

- Паролем може бути унікальна комбінація літер, цифр і спеціальних знаків або біометрична інформація: зображення обличчя (технологія Face ID) чи відбиток пальця (для пристроїв із Touch ID).

- Використовуйте біометричний захист у публічних місцях, це не дозволить шахраям підглядіти пароль до вашого телефону чи акаунту.

- **Довіряйте надійним джерелам інформації.**

- [Гайд](#), що розповідає про захист персональних даних.

- Інтерактивна [гра](#) для розвитку та покращення знань із кібербезпеки, яка зробить процес вивчення цікавим та легким для дітей.

Кампанія інформування громадян про кібербезпеку – важлива ініціатива, спрямована на підвищення рівня цифрової безпеки. Вона створена, щоб ознайомити людей із загрозами в інтернеті та просуванням правил безпечного перебування в онлайн-просторі.