

Безпека та гігієна в мережі



1. Комунікації в мережі.
2. Заходи безпеки.
3. Як перевіряти інформацію, яку споживаєш?
Маніпуляції в інтернеті.
4. Онлайн життя, репутація та цифровий слід.
5. Приватність в інтернеті. Параметри конфіденційності.
Практика налаштування приватності особистого
акаунту в соцмережах.

JLEU



Як користуватися інтернетом
безпечно та отримувати користь
від сучасних технологій та
застосунків?

JLEU



Інтернет — чудове місце для навчання і розвитку

- Можливо, у вас виникали питання про те, як безпечно користуватися інтернетом і отримати користь від сучасних технологій?
-
- Інтернет допомагає вам легко робити багато речей — купити нову шафу в два кліки чи теревенити зі шкільною подругою по відеозв'язку. Сьогодні комунікувати стало простіше. Повідомлення можна відправити, натиснувши на одну кнопку, а відповідь отримати вже через кілька хвилин.
- Онлайн-шопінг, дистанційне навчання, спілкування в інтернеті — всі ці речі для більшості людей звучать буденно, але, наприклад, людям старшого віку та людині з інвалідністю вони досі можуть бути недоступні.
- Спеціальні програми та мобільні застосунки дозволяють користуватися гаджетами та інтернетом без обмежень.

JLEU

Але навіть попри багато переваг інтернет спілкування, існують і певні ризики, тому все-таки необхідно пам'ятати про власну безпеку та правила комунікації в мережі. Також важливо знати кілька простих кроків, щоб убезпечити і себе, і своїх онуків в інтернеті.



Правила безпеки в інтернеті

Заходи безпеки під час користування смартфоном

Не передавайте смартфон стороннім. Якщо ваш телефон або планшет потрапить до рук зловмисника, він зможе користуватися вашим SMS-банкінгом, отримувати одноразові паролі для входу до вашого Банку та підтвердження платежів.

Захистіть свої смартфон і планшет від вірусів.

Щоб не заразити свій телефон вірусами:

- не зламуйте операційну систему свого смартфону та не проводьте банківських операцій через Інтернет на пристрої зі зламаню операційною системою;
- не відвідуйте незнайомі вам сайти;
- не переходьте за підозрілими посиланнями;
- встановлюйте програмне забезпечення тільки з перевірених джерел;
- під час встановлення додатків з App Store чи Play Market уважно ознайомтеся з дозволами, що запитують додатки;
- стежте за тим, щоб на вашому мобільному телефоні було встановлено та своєчасно оновлювалось антивірусне програмне забезпечення.



Безпечний пароль



Використовуючи надійний та сильний пароль, ви дбаєте про захист своїх облікових записів.

Пам'ятайте:

пароль для Facebook, Instagram, Telegram і т.д. має відрізнятися від паролів, які ви створили для входу в інші облікові записи, як ваша електронна пошта або банківський рахунок.

У якості пароля **не можна** використовувати адресу вашої електронної скриньки, номер телефону або дату народження.

Щоб залишатися в безпеці онлайн, пам'ятайте прості правила:

- Мисліть критично та будьте уважними.



- Не відкривайте повідомлень від невідомих номерів та із закликами перейти на невідомі сайти. Також будьте обережними з такими повідомленнями, як «Вам нарахована грошова допомога» з невідомих номерів.



- Захистіть свої соцмережі: встановлюйте складні паролі, не додавайте в друзі невідомі акаунти, увімкніть двоетапну автентифікацію.



- Не діліться з іншими паролями від своїх сторінок у соцмережах, не розповсюджуйте домашню адресу, номер телефону та банківські дані.



Ніколи не переходьте за сумнівними посиланнями, адже за ними може ховатися вірус або шахраї. Вони можуть використати ваші особисті дані в корисних цілях.

Підтримуйте «гігієну своїх пристроїв»: блокуйте пристрої щоразу після закінчення роботи, встановлюйте застосунки лише з офіційних сервісів, не користуйтеся невідомим **Wi-Fi**.

- https://www.flaticon.com/free-icon/lock_890132

JLEU



Як навчитися відрізняти правдиву інформацію від неправдивої або маніпулятивної інформації та завести звичку завжди перевіряти інформацію, яку споживаєш?

Як з першого погляду помітити ознаки неправдивої інформації?

Звертайте увагу на декілька характеристик:

- **1.** Наявність дуже великих чисел, сенсаційний характер новини або ж інформація відразу викликає дуже негативні емоції.
- **2.** Відірваність заголовка від змісту всієї новини. Цей прийом використовується для привернення уваги.
- Сама ж інформація в новині вже не така важлива. Тому потрібно читати як і заголовок, так і текст новини, щоб не допустити впливу фейків на себе.
- **3.** Дата, яка не відповідає дійсності. Часто старі публікації видаються за нові, тому рекомендуємо дивитися на дату новини або ж статті.
- **4.** Апелювання до надприродних речей та згадування відомих людей у невласивому для них контексті. Така інформація швидко поширюється та гарно запам'ятовується, бо суперечить нашим звичайним поглядам на життя.

Який алгоритм перевірки інформації на правдивість?

- Суть інструкції в тому, щоб ставити собі три прості запитання кожного разу, коли читаєте новини чи гортаєте стрічку в соціальній мережі.
- **1.** З'ясуйте першоджерело (автора) інформації.
- Якщо це інформація в соцмережах, перегляньте акаунт автора. Якщо автор публікації взагалі відсутній, такий інформації не потрібно довіряти. Якщо це новина чи стаття в ЗМІ, перевірте, чи має її автор ще якісь публікації і чи взагалі він існує.
- **2.** Перевірте, які аргументи наведені в тексті для підтвердження думки чи факту. Задумайтесь, а чи взагалі є підтвердження думки або факту в тій інформації, яку ви читаєте?
- Чи є посилання на джерело даних? Чи можна цьому джерелу довіряти? Наскільки правдиві дані, використані в публікації? Перевіряйте аргументи та пам'ятайте, що даними можна легко маніпулювати.
- **3.** Дізнайтесь, що говорять інші про це.
- Один з недоліків й одночасно одна з переваг інтернету — це надмірна кількість інформації, тому гарна ідея — дізнатися, що інші джерела говорять про цю тему.

Наскільки правдиві дані, використані в публікації?

Як розпізнати фейкові новини?

FAKE News erkennen

Сайти для перевірки фактів:

Mimikama – Zuerst denken, dann klicken

Correctiv

Tagesschau Faktenfinder

MedWatch

JLEU



Як захиститися від фішингу?

Крадіжка даних в Інтернеті

- **Фішинг** — це поєднання слів «пароль» і «рибалка» і означає перехоплення чи копіювання особистих даних та паролів електронною поштою, смартфоном або листом. Так звані ловці даних намагаються використовувати шахрайські методи для отримання інформації, щоб продати її з метою отримання прибутку.
- Тут ви можете дізнатися, які методи існують та як можна убезпечити себе:
<https://www.sparkasse.de/pk/ratgeber/sicherheit/was-ist-phishing.html>

Наприклад:

- Фішинг через СМС
- Фішинг текстових SMS-повідомлень, також відомий як смішинг, - це тип кібератаки, в якій використовуються SMS, що вводять в оману, щоб обманом змусити вас розкрити цінну інформацію. Наприклад, шахрай маскується під банк і надсилає текстове повідомлення з проханням оновити інформацію або перевірити щось в обліковому записі. Повідомлення зазвичай супроводжується загрозою – наприклад, якщо ви не виконаєте умови, ваш обліковий запис буде заблоковано.
- **SMS часто містить посилання на підроблений сайт, де необхідно ввести дані для входу. Це дозволяє шахраю отримати доступ до комбінації імені користувача та пароля.**
- Коли справа доходить до крадіжки у вас грошей, кіберзлочинцям потрібний **лише TAN**. Іноді вони навіть дзвонять зацікавленій особі, прикидаються співробітником банку та запитують.
- **Приклад Sparkasse**
- Sehr geehrte Kunde, Ihre registrierung fur di PushTan App läuft am 20.10.2023 ab.
- Jetzt ereuern:
[https://fake!](https://.....fake!)
- PushTan App – це відповідний додаток в якому генерується спеціальний код для підтвердження всіх операцій рахунку.
- Не слід просто натискати на посилання, чи то відомий чи невідомий номер.
- Важливо:
- Банки зазвичай не надсилають SMS-повідомлення. Навіть якщо ви хочете, щоб вам зателефонували з ощадної каси та домовилися <https://www.sparkasse.de/ratgeber/sicherheit/was-ist-phishing.html>
- Найкраще зателефонувати до відділення самостійно, перш ніж відповідати на вимоги до СМС.



JLEU



Як не стати жертвою маніпуляцій в інтернеті?

Проводячи час в інтернеті можна необачно потрапити у ситуації, які виявляються шахрайством. На перший погляд іноді їх не відрізнити.

Подивимося на наступні ситуації:

- Ви отримали електронний лист від когось, хто стверджує, що представляє відому організацію чи знаменитість, і повідомляє, що ви виграли велику суму грошей або приз.
- Ви нарешті знайшли в мережі оголошення того товару, який півроку не могли купити і вже готові його придбати, як-от продавець просить зробити передплату йому на картку.
- Ваш ліпший друг написав повідомлення в соціальній мережі з проханням терміново переказати гроші, розповідаючи про аварію, травми або арешт.
- Ми всі турбуємося про своїх близьких та рідних, але все частіше такі афери влаштовують після зламу електронної пошти користувача.
- Шахраї використовують інформацію зламаних облікових записів для того, щоб зібрати достатньо конфіденційної інформації, і надсилають досить



<https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSsMjZ-s5FTvW1eHBUh-uupikA0wyrEvkMKxF-Xpr25sw&s>

- переконливі запити про допомогу, щоб отримати кошти від небайдужих людей. На перший погляд іноді не відрізнити, що ви спілкуєтесь з іншою людиною, тому варто притримуватися простих рекомендацій, щоб бути в безпеці онлайн.

Крадуть фото з особистих сторінок користувачів: ще один вид шахрайства в соцмережах

У соцмережах помітили ще один вид шахрайства, у якому зловмисники використовують фото з особистих сторінок користувачів з Facebook, щоб виманювати кошти.

«Нова схема шахрайства: з Facebook завантажують фото аватарки і в Telegram заводять користувача з іменем та прізвищем, як у вас. Нічого при цьому не зламують. Далі шукають друзів з номерами телефону, які відкриті. Пишуть повідомлення типу «позич гроші». Дають картку. Чекають, поки ви «поведетесь».

Отримавши таке повідомлення, варто діяти розсудливо. Наприклад, спробувати зв'язатися з людиною, яка просить позичити кошти, зателефонувати їй, аби з'ясувати деталі.

Надсилати гроші лише тоді, коли ви встановили достовірність фактів і маєте підтвердження, що надіслане вам повідомлення справжнє.

Будьте максимально обачними, щоб не втратити кошти або ще й не наразити себе та свою родину на небезпеку!!

Що треба знати про безпечні покупки онлайн?

Купуючи щось онлайн, варто бути обережним, не передавати особисту та банківську інформацію, оскільки є великий ризик стати жертвою шахраїв.

Завжди намагайтеся використовувати онлайн магазини та сайти, які перевірені часом і популярні серед людей.



Безпечна вебсторінка магазину матиме «https://» і значок замка в адресі сайту — це гарантує захист даних покупця.

Фішингове посилання або посилання на інтернет-магазин, обов'язково в кінці має стояти буква **"s"** (**https://**). Якщо її немає — це означає, що сайт небезпечний.

Коли заходимо на сайт, потрібно звертати увагу, чи є якісь відмінності, орфографічні помилки навіть. Це не **100%**, що сайт шахраїв, але може так бути. Коли ми вносимо дані — обов'язково перевіряти, чи можуть ці дані бути використані проти вас і для того, щоб заволодіти вашими грошовими коштами.

Маркетплейси створюють власні сервіси для перевірки посилань на оголошення продавця.

Окрім великого вибору, у таких онлайн магазинів є внутрішні системи захисту користувачів, служба підтримки та послуги, які роблять шопінг безпечним, зокрема, перевірені методи оплати, зокрема онлайн-банкінг.

Або, наприклад, післяплата — це безпечний спосіб оплати, оскільки при оформленні замовлення на маркетплейсі та на сайтах компаній, покупець відразу оплачує **100%** його вартості.

А гроші перераховуються на рахунок продавця через **24** години після того, як покупець забере посилку у відділенні пошти.

Також придивіться до фотографій товару. Зазвичай порядні покупці знімають усе детально, щоб показати реальний стан товару та зацікавити покупця. Шахраї, як правило, не витрачають на це час і завантажують фото з інтернету.

Не соромтесь ставити питання про товар. У спілкуванні з продавцем завжди запитуйте все, що вас цікавить про товар, намагайтеся дізнатися якомога більше інформації.

● Не поспішайте з оплатою товару та не передавайте дані картки — номер картки та **CVV2**-код (три цифри на звороті картки). Якщо продавець видається вам підозрливим, ви можете повідомити про це службу підтримки онлайн-магазину.



**Пам'ятайте,
швидше за все, перед вами шахраї, якщо:**

- - ви бачите, що ціна на товар/послугу набагато нижча за ринкову.
- - продавець не дає повну інформацію про товар, квапить вас, але не відповідає на запитання.
- - вас просять надіслати повну інформацію про банківські картки чи рахунки.

Що робити, якщо ви стали жертвою шахрая в інтернеті?

Найгірше, що можна зробити – змиритися з тим, що вас обдурили і нічого не робити, щоб покарати зловмисників.

Цим ви тільки підсилите їхню віру у власну безкарність і активність.
Треба діяти навіть тоді, коли сума завданого збитку незначна.

Що ми радимо?

Якщо вас обдурили при покупці в інтернеті, заблокуйте свої картки і повідомте про випадок шахрайства мобільному оператору.

Також треба зв'язатися з кіберполіцією через форму зворотного зв'язку.

Обман стався з допомогою сайту-двійника?

Обов'язково скаржитесь на нього в **Google.**

Шахраює інтернет-магазин?

Пишіть скаргу на адресу продавця. Якщо претензію ігнорують, звертайтеся в поліцію.

Не треба думати, що власники інтернет-магазинів недосяжні для правосуддя: сайт знаходиться на хостингу, що передбачає наявність там точних паспортних даних власників.

Онлайн життя, репутація та цифровий слід

Потрібно пам'ятати: все, що ми пишемо та публікуємо в мережі, навіть у приватних повідомленнях, назавжди залишається в інтернеті.

Відповідально ставтеся до публікацій. Перш ніж натиснути «опублікувати», поміркуйте про зміст нового посту. Можливо, фото занадто особисте або текст можуть сприйняти неоднозначно.

Перед публікацією ще раз оцініть, чи може ця інформація будь-яким чином нашкодити вам або вашим близьким?

- Напевно з часом ми досягнемо точки, коли кожна людина матиме незручну інформацію та фотографії своєї юності, розміщені в соціальних мережах у Інтернеті.
- І компанії широко надаватимуть послуги з видалення інформації в мережі.
- Або ж ми користуватимемося правом змінити своє ім'я, щоб сховатися від незручного контенту про себе, з яким батьки ділилися в Інтернеті, коли їхні діти були підлітками.



- Колишній генеральний директор Google
- Ерік Шмідт

- https://uk.wikipedia.org/wiki/%D0%95%D1%80%D1%96%D0%BA_%D0%A8%D0%BC%D1%96%D0%B4%D1%82#:~:text=Eric%20Emerson%20Schmidt%3B%20%D0%BD%D0%B0%D1%80.,%D0%B2%D0%B8%D0%BA%D0%BE%D0%BD%D0%B0%D0%B2%D1%87%D0%B8%D0%BC%20%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BE%D1%8E%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%97%20Alphabet%20Inc.

Чому дописи у соціальних мережах про дітей можуть зашкодити їхньому майбутньому?



За даними дослідження інтернет-компанії AVG у 2010 році 81% дітей **у віці до двох років** мають у мережі цифровий профіль або цифровий слід, із їхніми зображеннями, розміщеними в мережі.



1) <https://www.youtube.com/watch?v=65jQAeVG5jk>

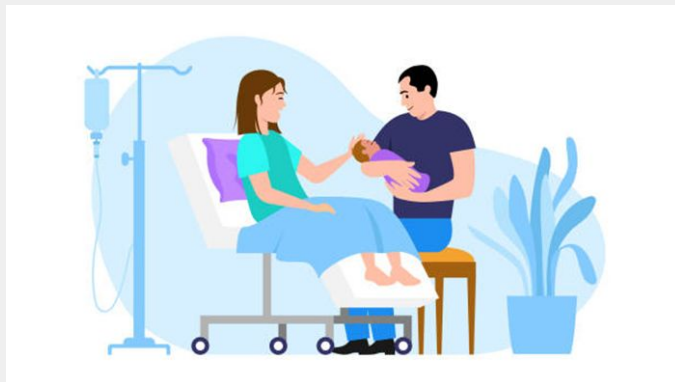
2)

https://media.istockphoto.com/id/930575966/uk/%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D1%96-%D0%B7%D0%BE%D0%B1%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F/%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%B0-%D1%96%D0%BB%D1%8E%D1%81%D1%82%D1%80%D0%B0%D1%86%D1%96%D1%8F-%D0%B4%D0%B8%D1%82%D0%B8%D0%BD%D0%B8-%D0%B7-%D0%BA%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D0%B5%D1%80%D0%BE%D0%BC.jpg?s=2048x2048&w=is&k=20&c=uMghbf_XZAQdsGr0psWblmGgcVIHyl-05Z9EVLwwrQU=

3) <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQIX25RVAnAraRzYycYMOxXYG4Aj98HUF5sG13XUDcAPIQpwAT36Nrh6TP3uQ7fTluCwek&usqp=CAU>

Особиста інформація

Перед публікацією в Інтернеті про себе, свою дитину чи онуку потрібно зупинитися й подумати, що це означає для життя, зокрема, дитини зараз і як це може вплинути на ваше життя та її подальше життя уже в дорослому віці?



Захистіть особисту інформацію, а також поговоріть з дитиною, онукою перш ніж ділитися фотографіями чи публікувати особисту інформацію про себе чи інших членів родини.

Особиста інформація містить **повні імена, дати народження, адреси, контактну інформацію або школу, в якій вони навчаються.** Потрібно бути обачним з цим, оскільки подібні деталі можуть використати зловмисники.

<https://media.istockphoto.com/id/1440559510/uk/%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D1%96-%D0%B7%D0%BE%D0%B1%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F/%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%B0-%D1%96%D0%BB%D1%8E%D1%81%D1%82%D1%80%D0%B0%D1%86%D1%96%D1%8F-%D0%B6%D1%96%D0%BD%D0%BE%D0%BA-%D0%BF%D1%96%D1%81%D0%BB%D1%8F-%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D0%B2-%D1%81%D1%86%D0%B5%D0%BD%D0%B0-%D0%BC%D1%83%D0%BB%D1%8C%D1%82%D1%84%D1%96%D0%BB%D1%8C%D0%BC%D1%83-%D0%B7-%D1%80%D0%B0%D0%B4%D1%96%D1%81%D0%BD%D0%BE%D1%8E-%D0%BC%D0%B0%D1%82%D1%96%D1%80%D1%8E-%D1%8F%D0%BA%D0%B0.jpg?s=612x612&w=0&k=20&c=vzo1VCvrgxMpuIDiuMdddC2nqOa-nHxDQYGexbCGc8=>

У соцмережах батьки дозволяють собі розкривати імена, вік та дату народження дитини зі своїх постів – наприклад, про святкування дня народження.

- Крім фотографій, батьки часто публікують домашні адреси; місто, де народилась дитина, дівоче прізвище матері, назви шкіл, імена домашніх тварин.
- Саме цю інформацію часто запитує банк при відкритті кредитної картки або її відновлення.
- Це може вплинути на фінансову безпеку дітей у майбутньому.



JLEU



https://media.istockphoto.com/id/1329127426/uk/%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D1%96-%D0%B7%D0%BE%D0%B1%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F/%D0%BC%D0%B0%D0%BB%D0%B5%D0%BD%D1%8C%D0%BA%D0%B8%D0%B9-%D0%B4%D0%B5%D0%BD%D1%8C-%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F-%D1%85%D0%BB%D0%BE%D0%BF%D1%87%D0%B8%D0%BA-%D0%B4%D0%BC%D0%B5-%D1%81%D0%B2%D1%96%D1%87%D0%BA%D0%B8-%D0%BD%D0%B0-%D1%82%D0%BE%D1%80%D1%82-%D0%B2%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BD%D0%B0-%D1%96%D0%BB%D1%8E%D1%81%D1%82%D1%80%D0%B0%D1%86%D1%96%D1%8F.jpg?s=612x612&w=0&k=20&c=S-pRHxpNrC0jRjIchTzNITYU-H_VmyvrPwdsDnvFE0=

Майбутня фінансова безпека

- До **2030** року пости в соціальних мережах про дітей призведуть до **2/3** випадків шахрайства з особистими даними, що коштуватиме людству сотні мільйонів доларів на рік.
- Маючи лише ім'я та дату народження, досить просто знайти інформацію про дитину, її фотографії та геомітки у **Facebook**.
- Злодії можуть зберігати цю інформацію, поки діти не почнуть відкривати банківські рахунки.



JLEU



<https://minfin.com.ua/img/2023/103924598/e7d6eae9a88f23e316723bb429386ab.jpeg?1681221932>

Нові можливості та нові загрози

Масова публікація фото власних дітей – не нове явище. 13 років тому з'явилося слово "**шеренінг**", яке складається з англійських слів **sharing та parenting**.

Крім очевидних проблем шеренінгу, таких як публікація фото дітей без їхньої згоди, не менш важливо, що батьки не сильно задумуються про конфіденційність власних акаунтів.

В умовах, коли технології ШІ переживають активний розвиток, контент з дітьми може використовуватися для створення так званого **Deepfake** – відео або аудіо, де люди говорять або роблять речі, яких вони ніколи не говорили чи не робили.

Це робиться за допомогою алгоритмів машинного навчання, які навчаються на величезній кількості даних.

Використання Deepfake з дитячим контентом найчастіше аморальне. Недавнє розслідування BBC показало, що за допомогою ШІ автори щомісяця можуть створювати тисячі зображень порнографічного характеру з дітьми різного віку.

Розміщують такий контент на іноземних сайтах, серед яких – популярна японська соцмережа Pixiv для любителів манги й аніме. Використання японської платформи дозволяє авторам залишатися поза юрисдикцією більшості країн Заходу, яка забороняє розміщення такого контенту. Та більше, порнографічний контент з дітьми часто створюється в комерційних цілях. Доступ до таких зображень коштує 3,85-8,5 дол на місяць.

На платформі Reddit, де раніше були опубліковані секретні дані про український контрнаступ, Forbes знайшов як мінімум 14 сабреддитів (форумів), де поширювалися порнографічні дипфейки.

Шеренінг може стати причиною крадіжки особистих даних дитини. Зловмисники можуть використати їх для шахрайства, обману кредиторів, подання заявки на державні пільги, купівлі авто в кредит, відкриття рахунків або оформлення кредитних карток. Найгірше, що батьки та їх дитина можуть дізнатися про це тільки після її повноліття.

Крім генерації візуального контенту, ШІ може імітувати людський голос.

Телекомунікаційна компанія Deutsche Telekom запустила соціальну рекламу про розміщення контенту в інтернеті. Ролик розповідає про імітацію голосу дитини.

https://www.youtube.com/watch?v=F4WZ_k0vUDM&t=1s

Злочинці почали використовувати ШІ для телефонного шахрайства, оскільки нова технологія дозволяє робити це більш витончено. Штучний інтелект за кілька хвилин може вивчити голос людини і почати його відтворювати.

ШІ здатен легко імітувати голоси відомих виконавців і створювати музичні композиції. Для музичної індустрії нові технології стають реальною загрозою в питаннях права власності. Google та найбільший у світі холдинг звукозапису Universal Music ведуть переговори про ліцензування мелодій і голосів виконавців для пісень, згенерованих ШІ.

Відповідно, якщо ШІ може створювати композиції з голосами зірок музичної індустрії, він запросто згенерує панічний голос конкретної дитини.

Така ситуація трапилася з американкою Дженніфер ДеСтефано, коли їй зателефонували з невідомого номера та голосом, повністю подібним до голосу її 15-річної доньки Бріанни, просила про допомогу та запевняв її про викрадення і вимагав 1 млн дол.

На щастя, через кілька хвилин ДеСтефано почула реальний голос своєї доньки, який запевнив її, що все гаразд.

Для США такий вид телефонного шахрайства стає дедалі частим явищем. За словами агента ФБР Шівона Джонсона, американські сім'ї у кожній фальшивій афері з викраденням втрачають 11 тис дол. За даними Федеральної торгової комісії, у 2022 році громадяни Сполучених Штатів втратили через шахрайство 2,6 млрд дол. У таких ситуаціях нереально перевірити, чи дійсно голос, який звучить під час розмови, належить члену сім'ї.

"Головне – не довіряйте голосу, який чуєте під час дзвінка. Якщо не можете зв'язатися з цією людиною, попросіть зробити це члена сім'ї або друга. Використовуйте кодові слова. Якщо хтось подзвонить і скаже, що викрав вашу дитину, ви можете запитати в дитини це слово", – радять у ФБР.

Правило білборду

Отже, Перш ніж **поставити лайк**, підписатися або прокоментувати, зупиніться і подумайте, чи хочете Ви чи ваші онуки, щоб це зображення або інформація відображалася, якщо хтось захоче шукати в інтернеті їх чи вас за іменем?

Використовуйте самі, а також у розмові з онуками правило білборду.

Уявіть, що ваш допис розмістили на великому білборді в місті. Чи комфортно, що всі бачитимуть це?

Публікуйте будь-що лише після схвальної відповіді дитини – це її перші кроки до розуміння згоди в цифровому середовищі.

Спілкування в соцмережах та онлайн-безпека для людей елегантного віку.

Приватність в інтернеті за допомогою параметрів конфіденційності

- Конфіденційність можна налаштувати як при реєстрації в соцмережі, так і пізніше.
- Варто бути обережним з тим, кому ви даєте можливість слідкувати за вашим акаунтом чи надсилати повідомлення в соцмережах.

Поради, за допомогою яких ви та ваші дані завжди будуть захищені

- Параметри конфіденційності на сайтах соцмереж допомагають контролювати те, що інші бачать на вашій сторінці.
- Окрім того, це забезпечує і вашу власну безпеку.
- Перейдіть у налаштування приватності та оберіть доступність ваших дописів і фотографій лише для друзів.
- Не додавайте в друзі незнайомих людей. Обов'язково переглядайте профіль людини, що доєднується до вас у друзі, і впевніться, що ви знайомі в реальному житті. Навіть якщо ви маєте багато спільних друзів, не варто підтверджувати запит від незнайомців.

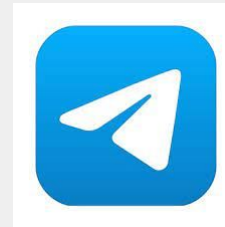


- Пам'ятайте:
 - людина, що додається в друзі під ім'ям та фото відомої особи на аватарці, — кетфішер, це той хто видає себе за іншого. Часто такі люди вигадують фальшиве минуле, роботу чи друзів, щоб повністю створити нову особистість.
- Якщо виникли сумніви щодо нового онлайн-знайомого, можна перевірити справжність його фотографії. Для цього, у браузері **Google Chrome** потрібно натиснути правою кнопкою миші на зображення, яке плануєте перевірити, та обрати опцію «Шукати» .

Практичні заняття

1. Відкрити приватну сторінку Телеграм.
2. Здійснити налаштування особистого акаунту.
3. Відкрити приватну сторінку Інстаграм.
4. Здійснити налаштування приватності особистого акаунту Інстаграм.
5. Здійснити налаштування приватності особистого акаунту у TikTok.

Налаштуйте приватність



- Як налаштувати приватність в соціальних мережах та месенджерах, ви можете дізнатися на прикладі **Telegram**
- це популярний у світі **Messenger**, який використовують як для спілкування, так і для перегляду різних так званих каналів сторінок із інформацією на відповідну тему: новини, спорт, технології тощо, оскільки саме в месенджерах ми опиняємося в великій кількості інформації, то при налаштування приватності варто ретельно подбати для цього
 - є сім простих кроків:
- **перейдіть налаштування та оберіть розділ приватність і безпека:**
- ❖ налаштуйте приватність вашого номеру **телефону**. Для цього у підрозділі приватність оберіть номер телефону встановіть, що ніхто не може бачити ваш номер телефону. Для того щоб його бачили окремі контакти оберіть «показувати для» та Додайте відповідних користувачів.
- ❖ «Профіль» доступний лише для ваших контактів. Для цього натисніть **на фото профілю** та оберіть мої контакти. Також ви можете приховати фото від певних користувачів додавши їх.
- ❖ Обмежте доступ користувачів то інформації про те, коли ви були онлайн: натисніть у розділі приватність категорію **відвідини** та стан у мережі, та оберіть, що ніхто не може бачити ваш час в мережі – ви, відповідно, теж не будете бачити час в мережі та останні відвідини інших користувачів. Для того щоб ця інформація показувалась для певних користувачів, наприклад для ваших друзів чи колег або членів родини, додайте їх до списку
- ❖ обмежте можливість невідомих користувачів **вам телефонувати**: оберіть в розділі приватність категорії виклики та оберіть, що **лише ваші контакти можуть вам телефонувати, або ніхто**
- ❖ влаштуйте **функцію переслання повідомлень**: поверніться до меню розділ «приватність і безпека» та оберіть у категорії пересилання повідомлень, що лише ваші контакти можуть переслати повідомлення разом із посиланням на ваш акаунт
- ❖ поверніться назад у розділ шосте обмежте людей, які можна **додавати вас у групи** та канали, навіть налаштування, перейшовши у цю категорію і «у групах та каналах» поставте, що лише ваші контакти можуть додавати вас до груп та каналів
- ❖ ви можете **блокувати** користувачів у розділі «приватність і безпека»: для цього натисніть на категорію «заблоковані користувачі» та Додайте до списку небажані контакти.
- **<https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSC8heyChC7b6qOjH7gqSHh72LOQaZFkjgL5XZSjWIKUc9Bq1-wayII1dYJXvysddpXSlo&usqp=CAU>**

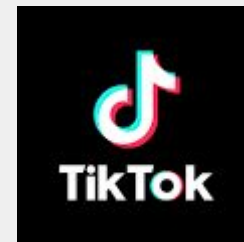
Як налаштувати приватність акаунту в **Instagram?**



- Як обмежити хейт спіч в Instagram?
- Як налаштувати приватність коментарів в Instagram?
- Як налаштувати приватність розповідей в Instagram та приховати свій мережевий статус?
- Як встановити двофакторну аутентифікацію в Instagram?
- Як налаштувати приватність дописів в Instagram?
- Як дізнатися, які данні про вас має Instagram?
- Як контролювати те, хто може надсилати вам повідомлення?

<https://www.youtube.com/playlist?list=PLo7hrBBCFI6NUktGUslt0l3VqHBhm84uo>

Про приватність у **TikTok**



- **TikTok** – сучасна інтернет мережа, де швидко зростає кількість користувачів, особливо віком **13-17** років. **TikTok** вже скачали близько **2** млрд разів.
- **Що про мене знає ТікТок?**
- **Як встановити двоетапну перевірку в ТікТок?**
- **Як налаштувати приватність акаунту в **TikTok**?**
- **Ви хочете, щоб Ваші відео та вашої дитини бачили лише її друзі та знайомі?**
- Налаштуйте приватність акаунту, для цього достатньо зробити лише декілька кліків:
- <https://www.youtube.com/watch?v=PTpEXSVo4tQ&list=PLo7hrBBCFl6NJrauigY9eZ0yBR3uKmlno&index=3>
- <https://p16-va-tiktok.ibytemg.com/obj/musically-maliva-obj/13fefb5b6fc913bce285cf4ee6e0611d>

Як обмежити дані, які про мене збирає Фейсбук?



- <https://www.youtube.com/watch?v=6sBuejKdJbM&list=PLo7hrBBCFl6M6qcqSsYPStTLrTthKs5DK&index=6>

JLEU



**Мобільні додатки,
які повинен мати кожен житель
Німеччини**

Додаток-попередження NINA BVK

(Федеральне відомство з надання допомоги при стихійних лихах цивільного захисту)



- NINA - це корисний інструмент, призначений для повідомлення резидентів Німеччини про будь-які надзвичайні ситуації, що насуваються, або катастрофи в реальному часі.
- Завдяки простому інтерфейсу, будь-який користувач програми може отримувати офіційну інформацію щодо всіх природних лих, подій та інших ситуацій, які можуть наразити на ризик життя людей. Додаток попереджає про небезпечні ситуації, такі як наприклад теракт. Під час пандемії додаток в основному використовувався для поширення важливої інформації та офіційних інструкцій щодо коронавірусу.
- Щоб NINA могла правильно визначати можливі ризики, необхідно надати їй доступ до інформації про ваше місцезнаходження. Тоді вона зможе визначати, в якому районі Німеччини ви перебуваєте, і повідомлятиме про все, що відбувається в цьому районі.
- Щоб скористатися безкоштовними послугами цього додатка, вкажіть область, про які хочете отримувати повідомлення.
- Основні функції такі:
- ☐ Попереджувальні повідомлення цивільного захисту з рекомендаціями до дії.
- ☐ Прогноз погоди Deutscher Wetterdienst (DWD) для всієї Німеччини або за районами.
- ☐ Інформація про повені.
- ☐ Загальні екстрені поради, щоб ви могли захистити себе та інших від можливих небезпек.

https://www.nuernberg.de/imperia/md/zentral/bilder/fittosize_570_380_017545e50936e2b51dc8e42b4c7b00a4_smartphone_nina_app.jpg

nora - офіційний додаток для екстрених викликів федеральних штатів.



- Якщо ви або інші особи потрапили у Німеччині в надзвичайну або небезпечну ситуацію та потребуєте швидкої допомоги з боку поліції, пожежної служби чи рятувальної служби – додаток допоможе!
- За допомогою безкоштовної програми екстреного виклику Nora ви можете звернутися безпосередньо до відповідальних центрів управління поліції, пожежної частини та рятувальної служби - так само, якби вам зателефонували за номерами екстреної допомоги 110 або 112.
- Коли і як можна використовувати застосунок nora, щоб викликати допомогу у надзвичайній ситуації показано у цьому відео:

<https://www.nora-notruf.de/pictures/W1siZiIsIjIwMjEvMDcvMDIvNWY4ZnpzaWt6aV90ZWxlGhvbmlVfbm9yYV9hcHAuc3ZnIl1d/telephone%20nora%20app.svg?basename=telephone+nora+app&sha=41889d44e889f6bd>

<https://www.nora-notruf.de/en-en/nora-video-ukrainian>