

10 ПОРАД

**ДЛЯ ЗАХИСТУ
ВІД ІНФОРМАЦІЙНИХ
МАНІПУЛЯЦІЙ**

**НЕ ДАЙ ВВЕСТИ
СЕБЕ В ОМАНУ**

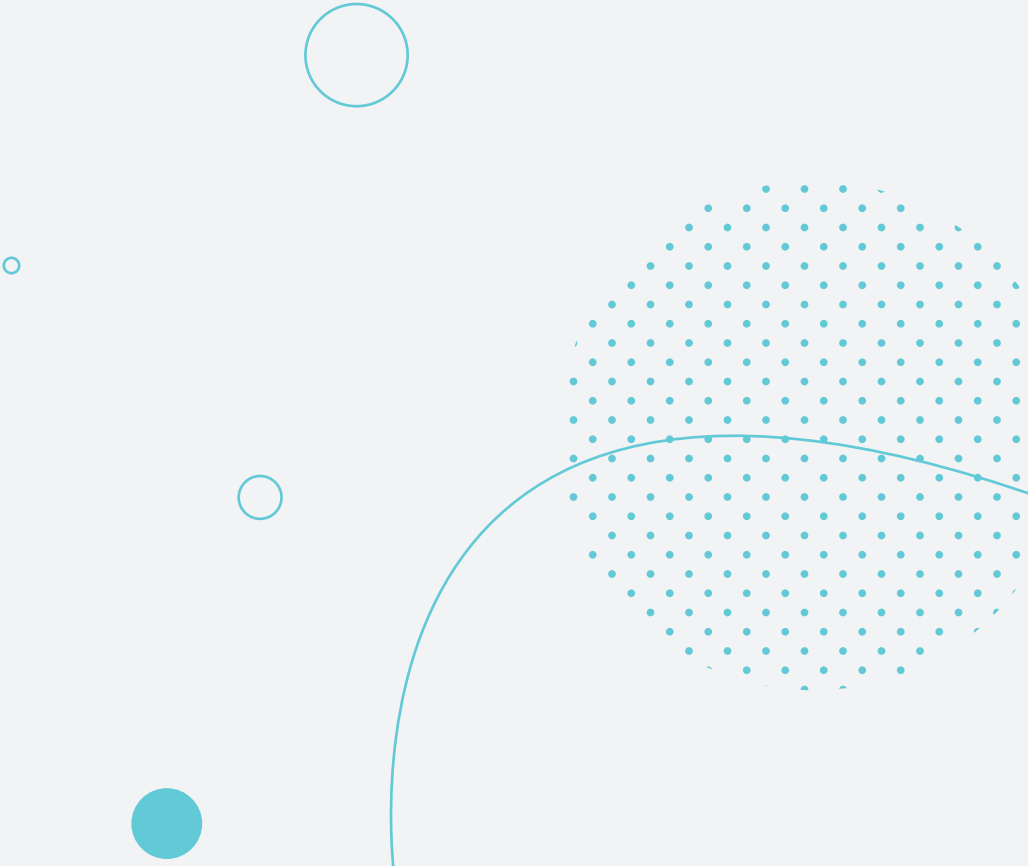




У сучасному буремному інформаційному світі дуже легко стати жертвою маніпуляцій. **Маніпуляція** – це приховане управління людьми та процесами, зокрема через інформаційні інструменти.

Ми підготували **10 порад**, які можуть захистити вас від цих маніпуляцій.

Ці поради ґрунтуються на онлайн-курсі **«Інформаційна безпека»**, що його 2021 року створила ГО «Інтерньюз-Україна» за підтримки Центру інформації та документації НАТО в Україні. Якщо хочете дізнатися більше, запрошуємо на цей курс на платформі Prometheus. Докладнішу інформацію можна знайти на *internews.ua*.



1 ДОВІРЯЙТЕ, АЛЕ ПЕРЕВІРЯЙТЕ

Довіра – ключова чеснота суспільства. Без довіри суспільства не існує. Одна з великих проблем сучасних суспільств (не лише українського) – **низький рівень довіри**. Часто нам здається, що хтось хоче ввести нас в оману, обдурити чи навіть знищити.

Довіру варто випрацювати. Але вона **не має** ставати сліпою вірою. Тому в довірі завжди має бути компонент **критичного погляду** й перевірки. Між абсолютною довірою та абсолютною недовірою треба щоразу знаходити баланс. Це й означає: довіряйте, але перевіряйте. Якщо через прості процедури перевірки інформації ви бачите, що цій інформації або цьому джерелу довіряти не варто, значить, не довіряйте їм. Якщо ж інформація збалансована, добре аргументована, враховує різні позиції і не містить емоційних маніпуляцій, можливо, їй варто довіряти. Хоч і обережно.

довіра

критичний погляд

- перевірка інформації
- баланс думок
- достовірність
- точність
- повнота
- відокремлення фактів від коментарів
- аргументація
- різні позиції
- відсутність фейків та маніпуляцій

~~сліпа віра~~

2 ЗРОЗУМІЙТЕ, КОЛИ ЕМОЦІЇ ДОПОМАГАЮТЬ, А КОЛИ – ШКОДЯТЬ

Емоції можуть бути позитивними й негативними, можуть нести любов чи ненависть, відчуття єдності чи відчуття війни. Велике завдання – зрозуміти, коли вони допомагають нам, а коли – шкодять. Емоції можуть бути шляхом до **співпереживання**, а можуть викликати бажання **вбити чи знищити**.

Ділянки мозку, які відповідають за емоції, формувалися під час найдавніших початків нашої еволюції. Вони були – і є нині – системою попереджень та задіяння миттєвих реакцій: передусім для того, щоб **уникати небезпеки**. А тому «емоційні» виміри процесів нашого мозку швидші за «раціональні» виміри. Вони захоплюють увесь наш мозок, «усе наше єство», аби не дати проникнути іншим думкам та іншим елементам.

Дуже часто в нашій узаємодії з інформацією емоції заважають нам подивитися на реальність із багатьох сторін. У цьому сенсі емоції можуть звужувати нашу перспективу.

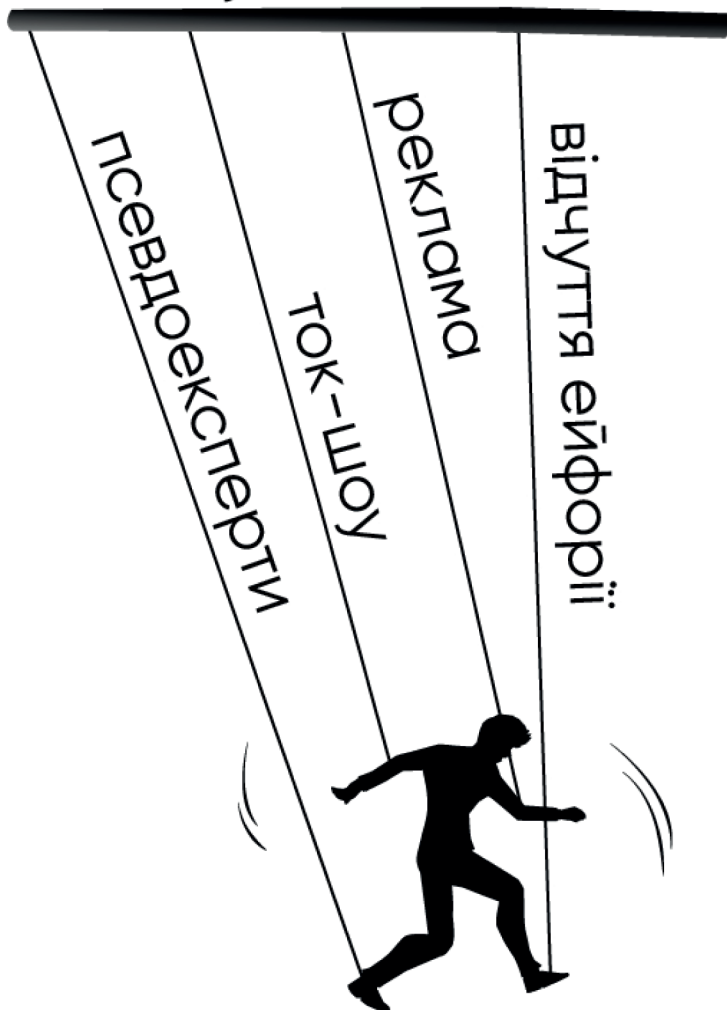
Тому важлива порада: будь-яку **інформацію, яка викликає емоцію, потрібно відправити на карантин**. Дати собі час заспокоїтися, емоціям – ушухнути, а тоді вкотре перечитати її і спробувати відділити зерна від половини.

Ось чому не варто ухвалювати важливі рішення у стані ейфорії – появі відчуття потрібності, важливості, цінування тощо. Маніпуляції в рекламі, як правило, ґрунтуються на психологічних особливостях людини. Тому протистояти їм дуже важко.

Також якщо ви любите такі медійні продукти, як ток-шоу, будьте з ними обережні. Ток-шоу часто прагнуть **маніпулювати вашими емоціями**. Тому не сприймайте на віру все, що розповідають або показують у них. Перевіряйте озвучені факти, якщо вони викликали у вас подив чи обурення. Найшвидше це можна зробити в інтернет-джерелах, тож просто погугліть цифру, цитату або ім'я незнайомого вам експерта. Пам'ятайте, що найбільше довіри у вас викликають політики й експерти, яким ви симпатизуєте. Але навіть їхні твердження потрібно **перевіряти**. Ніхто не ідеальний. Зверніть увагу, хто з учасників ток-шоу говорить найбільше і найемоційніше. Можливо, саме він або вона дезінформують, граючи на емоціях. І, нарешті, не покладайтесь на реакцію аудиторії в залі. Завжди майте власну думку й власне ставлення до людей, подій та фактів.

За матеріалами Тетяни Матичак, Альони Романюк
та Володимира Єрмоленка

маніпуляції емоціями



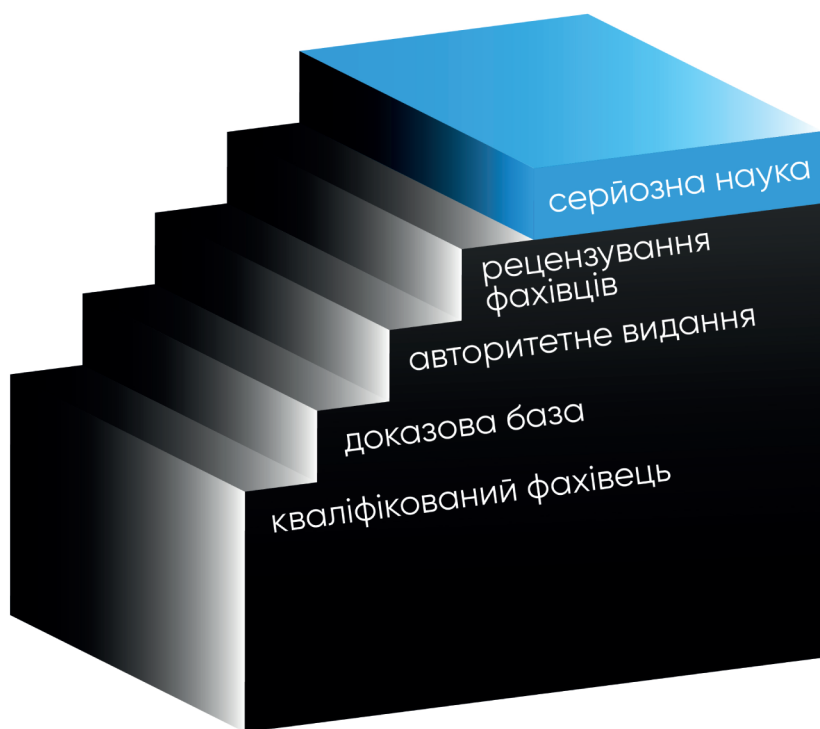
3 ДОВІРЯЙТЕ СЕРІОЗНІЙ НАУЦІ

Наукові висновки можуть робити лише науковці. Тому:

- перевірте, чи пораду дає **кваліфікований фахівець**, який/яка має серйозну репутацію в своїй сфері та/чи працює в інституції, що має таку репутацію;
- піддавайте **сумніву** твердження, доведені лише загальними фразами на кшталт «учені довели». Немає ніяких «учених узагалі»: є конкретні дослідники, які доходять конкретних висновків, що їх підтверджують або не підтверджують інші дослідники;
- перевірте **авторитет** науковця серед його/її колег, пошукайте її/його наукові публікації – їх має бути надруковано в авторитетних журналах;
- пам'ятайте: астрологія, екстрасенсорика тощо – це **не науки**! Вони належать до сфери забобонів і первинних вірувань.

Пам'ятайте, що існує низка маніпуляцій довкола нерецензованих досліджень. Є сайти, на яких вчені публікують власні дослідження і разом з іншими науковцями дискутують, аргументують свою позицію, а часом, коли розуміють, що припустилися помилки, видаляють свої матеріали. Проте журналісти й медіа видають цю інформацію за правдиву і в такий спосіб вводять нас в оману. Дослідженню можна довіряти, якщо воно проходить **рецензування інших фахівців** і опубліковане в авторитетних виданнях.

За матеріалами Тетяни Матичак і Альони Романюк



4

ДРУЗІ І ЗНАЙОМІ – НЕ ЗАВЖДИ ЕКСПЕРТИ; СОЦМЕРЕЖІ – НЕ ЗАВЖДИ ДЖЕРЕЛО

Наші друзі та знайомі – джерело наших великих радостей і приємних емоцій. Найближчим людям треба і варто довіряти, з ними треба спілкуватися, допомагати їм, але вони **не є** експертами в усьому. Не варто вірити інформації, яку поширює людина, тільки тому, що ви її добре знаєте. «Хороша людина» – не професія, і люди можуть помилятися з найкращих намірів: просто тому, що чогось не знають.

Чимало **соціальних мереж** немовби замінюють нам друзів і знайомих. Ми занадто довіряємо тим, з ким чатимосся, і це може бути небезпечно.

Зверніть увагу, наприклад, на чати і групи у Viber. Колись ми спілкувалися з рідними за допомогою SMS і телефона. Потім з'явився Viber, і все стало набагато зручніше й безкоштовно. Згодом коло спілкування в месенджері розширилося: до нього ввійшли колеги, сусіди тощо. Проте це були знайомі люди. Тому за цим месенджером і закріпився штамп **«тут усі свої»**. Тож щойно з'являється важлива, корисна, сенсаційна чи просто цікава інформація, нею щедро з усіма діляться. Бо про безпеку передусім потрібно попередити своїх. І про лайфхак, що спрощує чи рятує життя, теж.

Viber ставав популярнішим, і дуже скоро наше коло спілкування в ньому розширилося і на геть незнайомих людей, і на звичайних ботів. Проте штамп «усі свої» залишився. Він і лежить в основі поширення фейків.

Достатньо приписати до повідомлення «попередь усіх» чи «перешли, бо цю інформацію всюди видаляють», як лавину повідомлень не зупинити. Силу Viber показала пандемія коронавірусу. Безпека й здоров'я – це саме та інформація, яку миттєво поширюють у месенджері.

Щоб захиститися від маніпуляцій, перевірте налаштування і переконайтеся, що вас не можна додавати в чати або спільноти без вашої згоди. Для конфіденційного спілкування вибирайте надійні месенджери (наприклад, Signal). Не забудьте встановити надійний та унікальний пароль і двофакторну аутентифікацію. Перш ніж підписатися на канал, перевірте його автора чи медіа. Переконайтеся, що це справді їхній канал.

За матеріалами Оксани Мороз та Володимира Єрмоленка

Можливі ознаки маніпуляцій



5

БУДЬТЕ УВАЖНІ ДО ФОТО І ВІДЕО

Коли ми бачимо фото чи відео, нам одразу може здатися, що це факт. Адже це візуальний матеріал, який ідеально відтворює подію, особу, предмет, місце тощо.

Але фото й відео сьогодні є джерелом величезної кількості маніпуляцій. Ось декілька типів маніпуляцій, з якими стикаємося у візуальному контенті.

Перший тип фото- чи відеофейку – це підробка, яка здійснюється в момент знімання.

Скажімо, 2015 року в соціальних мережах активно поширювали фотографію із зображенням хлопчика на тлі зруйнованих будівель. У підписі до фотографії стверджувалося, що замурзаний хлопчик із Донецька шукає свою «матір серед руїн розбомбленого ВСУ дому». Насправді ця фотографія – кадр із відеокліпу «Янгол. Пісня про дітей Донбасу», в зйомках якого брала участь ця дитина. Маленькі актори – хлопчик і дівчинка – нібито шукали допомоги. Фактчекери виявили, що їхні батьки живі.

Другий тип – редагування зображень у спеціальних фото- або відеопрограмах. Наприклад, 2020 року користувачі соцмереж поширили світлину британської королеви Єлизавети II в українській вишиванці. Всі активно дякували королеві й раділи. Та перевірка фотографії показала, що на оригінальному фото – королева в бірюзовому вбранні, а не у вишиванці. Зверталася королева до британців у зв'язку з пандемією COVID-19.

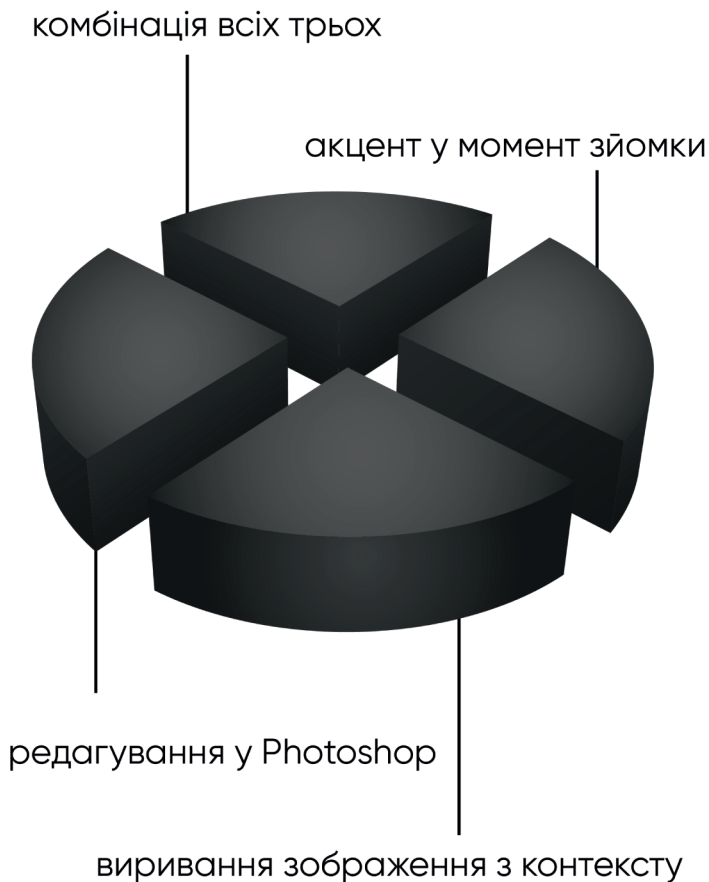
Третій і найпоширеніший – це виривання фотографії з контексту. Тобто коли реальні фото або відео, відзняті в одних обставинах, ілюструють зовсім іншу історію. Скажімо, серед української аудиторії Facebook поширювалося відео міста, що його накриває хвиля води. Підпис повідомляє, що в Китаї прорвало дамбу і вже сто тисяч людей загинуло. Насправді на відео – цунамі в Японії у 2011 році.

І **четвертий**, найскладніший – це поєднання всіх названих типів, коли зображення і домальовують, і маніпулятивно вписують у неправдивий контекст.

Висновок: пам'ятайте про всі можливі маніпуляції. І не вірте сліпо всім фото і відео, які бачите.

За матеріалами Вікторії Романюк

Маніпуляції фото та відео





ПАМ'ЯТАЙТЕ: ФЕЙКИ ПРО ЛІКИ МОЖУТЬ УБИВАТИ

Фейки про ліки і способи лікування можуть убивати. Проте стає занадто пізно, коли людина розуміє, що повелася на брехню. Пам'ятаймо декілька речей:

- Фейки виникають там, де є брак інформації та підвищений попит на тему.
- Фейки й маніпуляції швидко поширюються, коли тема стосується життя, здоров'я та особистої безпеки людини. Тому з повідомленнями на такі теми треба бути дуже обережними.
- Інформація, яку надсилають у месенджерах, часто не має достовірного джерела або надходить до вас у спотвореному вигляді. Їй не варто вірити.

Головне правило: **не поширюйте** повідомлення, якщо ви не впевнені у його достовірності. Не поширюйте повідомлення або пост, якщо це перше бажання, яке виникає у вас після його прочитання.

Які ж типи дезінформації на медичні теми (передусім коронавірус) ми сьогодні бачимо?

Перший тип дезінформації – це конспірологічні фейки й **теорії змови**. Простіше кажучи, це повідомлення і тези, що пояснюють коронавірус, вакцинацію та запровадження карантинних обмежень як результат таємного плану впливових людей або організацій.

Такі фейки поширювали як псевдоексперти, так і народні депутати, політтехнологи, блогери й медіа. Унаслідок дезінформаційної кампанії 66% українців вважають, що коронавірус має штучне походження, хоча **доказів цього немає**.

Другий тип дезінформації стосується ефективності лікування коронавірусу різними лікарськими засобами. Треба розуміти, що ліки, які застосовують медики по всьому світу, впливають тільки на полегшення симптомів. Відповідно, всі повідомлення про ефективність тих чи інших засобів – це фейк або маніпуляція. Самолікування та вживання антибіотиків, протималарійних або серйозних антивірусних препаратів може дуже нашкодити здоров'ю. Саме тому не варто купувати в аптеці перші-ліпші препарати, що їх рекламують як ліки від коронавірусу.

Третій тип дезінформації – це фейки та маніпуляції про методи профілактики й лікування коронавірусу.

Повідомлення і матеріали про користь народних та альтернативних методів подолання COVID-19, на жаль, нерезультативні. Уринотерапія, вживання алкоголю, імбиру, часнику та інших домашніх засобів не вилікують вас. А от зашкодити можуть.

За матеріалами Альони Романюк

пігулки від інфодемії

імунітет до теорій
змови про коронавірус

народні засоби не
лікують коронавірус

альтернативна медицина не
допоможе при коронавірусі

7

ОСТЕРІГАЙТЕСЯ БОТІВ І ТРОЛІВ

Соціальні мережі дають чимало переваг. Але в них є не лише ваші друзі та родичі, а й **боти, тролі та зловмисники**.

Бот – це спеціальна програма, що виконує автоматично і за заданим розкладом які-небудь дії через ті ж інтерфейси соцмереж, що й звичайний користувач.

На відміну від ботів, **тролі** – це справжні люди, які сидять у мережі під фейковими акаунтами. Вони можуть ображати інших користувачів або їхні переконання, провокувати їх на конфлікт і всіляко уникати конструктивної бесіди.

У сучасному середовищі дедалі більше застосовується **комбінований підхід**: використання бота й людини водночас. Ботоферми – це групи людей, що фізично працюють із великою кількістю ботів. Через спеціальні інтерфейси люди лайкають, коментують і поширюють пости з багатьох акаунтів і за це отримують невелику платню.

Як **ідентифікувати** ботів і тролів?

По-перше, боти і тролі дуже часто не мають **аватарки** або ж замість звичайного фото використовують абстракцію чи картинку.

Ще одна важлива ознака бота чи троля – **відсутність власного контенту** й публікацій.

Замість цього такі акаунти роблять регулярні репости контенту з інших сторінок або ж узагалі не мають дописів.

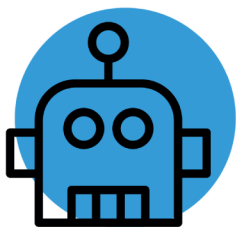
Окрім того, боти постануть у коментарях велику кількість **зовнішніх посилань** на сторонні сайти. Варто пам'ятати, що боти в середньому використовують посилання втричі частіше, ніж люди. На те, що акаунт є ботом чи тролем, також може вказувати неспівмірність між датою реєстрації та кількістю публікацій. Скажімо, якщо акаунт зареєстровано місяць тому, а він уже має декілька сотень публікацій, – це підозріло.

Стежте за **годинами активності** акаунтів. Якщо вони зареєстровані у США, але постануть удень за московським часом, тут щось не те.

Водночас пам'ятайте, що боти й тролі можуть дуже вдало маскуватись, а реальні люди – поводитися дивакувато. Тому ці правила не є універсально застосовними: до кожного акаунта потрібен індивідуальний підхід.

За матеріалами Віталія Рибака

Можливі ознаки бота



велика кількість
зовнішніх посилань
в коментарях



публікація одного
і того ж коментаря



відсутність
власного контенту,
регулярні репости

забагато
публікацій



немає аватару
чи абстракція
замість фото

дуже часті
публікації



недостовірна або зовсім
не заповнена інформація
в профілі



БУДЬТЕ ОБЕРЕЖНІ, КОЛИ ВИ ОНЛАЙН

Світ технологій відкриває нам безліч можливостей, а водночас і загроз. Він робить наше спілкування швидшим і простішим, але й створює безліч додаткових вразливих точок, через які ми можемо стати жертвами зловмисників.

Як уберегтися від атак зловмисників онлайн? Ось **декілька порад**:

- завжди пам'ятайте про те, що вас можуть атакувати. А тому будьте уважні до можливих загроз;
- не додавайте в друзі людей, не відомих вам;
- намагайтеся не розголошувати номер вашого мобільного;
- якщо вам погрожують, надсилайте скаргу адміністрації соцмережі, блокуйте користувача й звертайтеся до кіберполіції;
- користуйтеся безпечними месенджерами (наприклад, Signal значно безпечніший за Viber);
- користуйтеся опцією «подвійної аутентифікації»;
- надійно зберігайте свої паролі – скажімо, за допомогою спеціальних програм.

Особливу небезпеку становлять так звані **«фішингові»** листи.

Це листи, які містять зловмисний елемент, що може вам нашкодити: заразити комп'ютер вірусом, викрасти дані тощо.

Зазвичай фішинг практикують через мейл. В електронному листі зловмисники здатні:

- надіслати вам підроблений лист, дезінформувати або змусити щось зробити. Для прикладу, видаючи себе за вашого колегу, попросити вас передати чутливі дані: документи, паролі та інше;
- відправити посилання, що вестиме на підроблений сайт, де у вас можуть украсти пароль;
- додати в електронний лист зловмисну програму.

Ці зловмисні листи можуть потрапити у папку «вхідні» (а не у спам). А це означає, що тільки від вас залежить, чи зможете ви розпізнати такий лист і правильно зреагувати – видалити його.

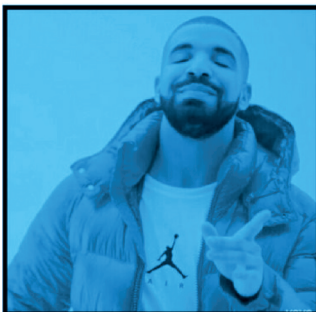
Саме тому вам потрібно засвоїти такий алгоритм дій:

- ретельно перевірити електронну адресу відправника – чи це справді лист із адреси вашого банку, а не з подібної адреси;
- перш ніж натиснути на кнопку чи посилання, наведіть на них мишкою, щоб побачити, на який сайт вони ведуть;
- не відкривайте файлів одразу, а перевіряйте їх на сайті [virustotal.com](https://www.virustotal.com).

За матеріалами Віталія Мороза та Павла Белоусова



додавати в друзі невідомих
пароль qwerty12345
розголошувати
номер мобільного
відкриті мережі Wi-Fi



безпечні месенджери
подвійна аутентифікація
менеджери паролів
захищені браузері



БУДЬТЕ ПИЛЬНІ З ЦИФРАМИ

Оперування цифрами часто створює ілюзію «залізних аргументів». І саме тому цифрами так часто маніпулюють. Тож, працюючи зі статистичною інформацією чи соціологічними даними, варто пам'ятати декілька важливих правил.

- Довіряти варто лише **офіційній інформації**. До надійних джерел належать вебсайти державних інституцій (Державної служби статистики, Національного банку України, Міненерго, Нафтогазу, Міністерства фінансів, Держказначейства, Пенсійного фонду тощо).
- Дані мають давати **повну картину** про явище. Якщо статистика описує подію в повністю позитивному чи повністю негативному світлі, цілком імовірно, що це фейк. Адже односторонність – один із улюблених інструментів маніпуляторів.
- Стежте за **порівнюваністю даних**. Скажімо, порівняння зарплат і решти доходів у доларах не є правильним, оскільки національна валюта України – гривня, а не долари. Окрім того, при такому порівнянні завжди треба враховувати інфляцію.
- Якщо ви сумніваєтесь у трактуванні і використанні статистики, запитайте фахівців. Проте не всі люди, які називають себе експертами, насправді є ними. Перш ніж довіряти думці фахівця, необхідно перевірити його **освіту, спеціалізацію та репутацію**, а також подивитися на його риторику в медіа й соціальних мережах.

Також пам'ятайте: соціологія – це наука. Довіряйте тільки перевіреним науковцям.

Якщо говоримо про соціологічні дослідження, знайдіть відповіді на такі запитання:

- **Хто** проводив опитування? Це перевірена компанія? Чи це фірма, яку було створено «під вибори»?
- **Кого** опитували? Це вибірка, яка відображає зріз населення України, чи дослідження лише однієї вікової чи професійної категорії?
- **Коли** проводилось опитування? Наприклад, 1 квітня 2020 року в Україні розпочалася медична реформа. Тож якщо опитування щодо задоволеності лікарів реформою проведено у травні, воно не покаже реального ефекту від запроваджених змін.
- **Як** сформульовано запитання? Від формулювання запитання залежить і відповідь на нього. Наприклад, понад 70% українців на запитання «Чи варто зняти мораторій на продаж сільгоспземель?» відповідали: «Ні, не потрібно». Однак на запитання «Чи повинен власник паю мати право розпоряджатися ним, у тому числі продати?» майже така ж кількість респондентів відповідала: «Так, повинен». Хоча фактично запитання були про одне й те ж: відкриття ринку землі.

За матеріалами Світлани Сліпченко



10

РОЗУМІЙТЕ, ЯК ПРАЦЮЄ ІНТЕРНЕТ

Фейки, дезінформацію та маніпуляції спрямовано на те, щоб сформувати у вас хибну картину світу. Вони можуть стосуватися абсолютно різних сфер життя. Чи не найбільший канал їх поширення – інтернет.

Скажімо, на результат пошуку у відомих пошуковиках, наприклад, Google, передусім впливає **мова**. Якщо мова запиту **російська**, ключові посилання будуть на російські медіа з їхніми наративами. Це зумовлено роботою алгоритму: згори сторінки показують популярні посилання, тобто ті, на які переходить велика аудиторія.

Також чималу роль відіграє наша **історія пошуку**. Тобто якщо ви полюбляєте читати новини із сайтів-сміттярок, пошуковик робитиме висновок, що для вас це оптимальний інформаційний ресурс, і добиратиме подібні.

Кожна **наша дія** в інтернеті має наслідки. Google чудово це ілюструє. На результати нашого пошуку впливає те, що ми шукаємо в суміжних сервісах (YouTube, Gmail), що пишемо в месенджерах та інших сервісах цієї корпорації. Усі її послуги інтегровані, щоб максимально вивчити нас, і, зважаючи на це, безпосередньо формувати оптимальний, з погляду Google, набір матеріалів.

Звісно, вплив має наша залученість у матеріал: як довго його читаємо, поширюємо чи пересилаємо це посилання тощо.

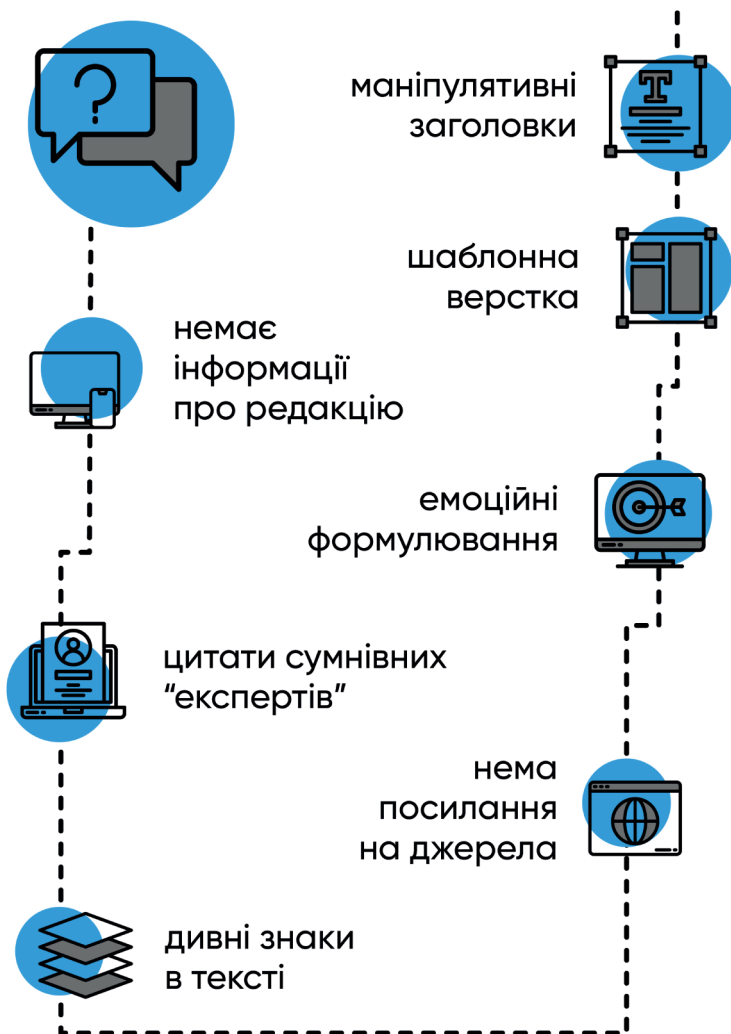
Як наслідок, на першій сторінці пошуку ми отримуємо традиційний для цифрових платформ «оптимальний набір», створений **персонально під нас**. Тож результати пошуку тієї самої інформації в різних користувачів будуть різні.

Якщо ви шукаєте інформацію з неконфліктної теми, наприклад «Як спекти пиріг», то просто отримаєте результати роботи алгоритму Google. Проте, шукаючи інформацію з конфліктної чи потенційно конфліктної теми, з великою часткою імовірності матимете ті результати, які заклад маніпулятор.

Щоб уберегтися від маніпуляцій, необхідно **розуміти першоджерела**. Якщо ви вивчаєте нову для себе й вузькопрофільну тему або першоджерела іноземною мовою зі складною термінологією, варто звернутися до об'єктивних вторинних джерел: медіа або експертів. Проте прискіпливо їх перевіряйте. Святих медіа чи джерел інформації не буває. Усі можуть помилятися. Перевіряйте отриману інформацію, зіставляючи її з даними з інших джерел.

За матеріалами Оксани Мороз

Ознаки «сайтів-сміттярок»





Цей посібник ґрунтується на матеріалах онлайн-курсу «Інформаційна безпека», що його 2021 року створила ГО «Інтерньюз-Україна» за підтримки Центру інформації та документації НАТО в Україні. Із курсом можете ознайомитися на платформі Prometheus.

У посібнику використано матеріали експертів із дослідження інформаційного поля та дезінформації, які взяли участь у підготуванні курсу. Це Павло Белоусов, Володимир Єрмоленко, Тетяна Матичак, Віталій Мороз, Оксана Мороз, Віталій Рибак, Альона Романюк, Вікторія Романюк, Світлана Сліпченко.