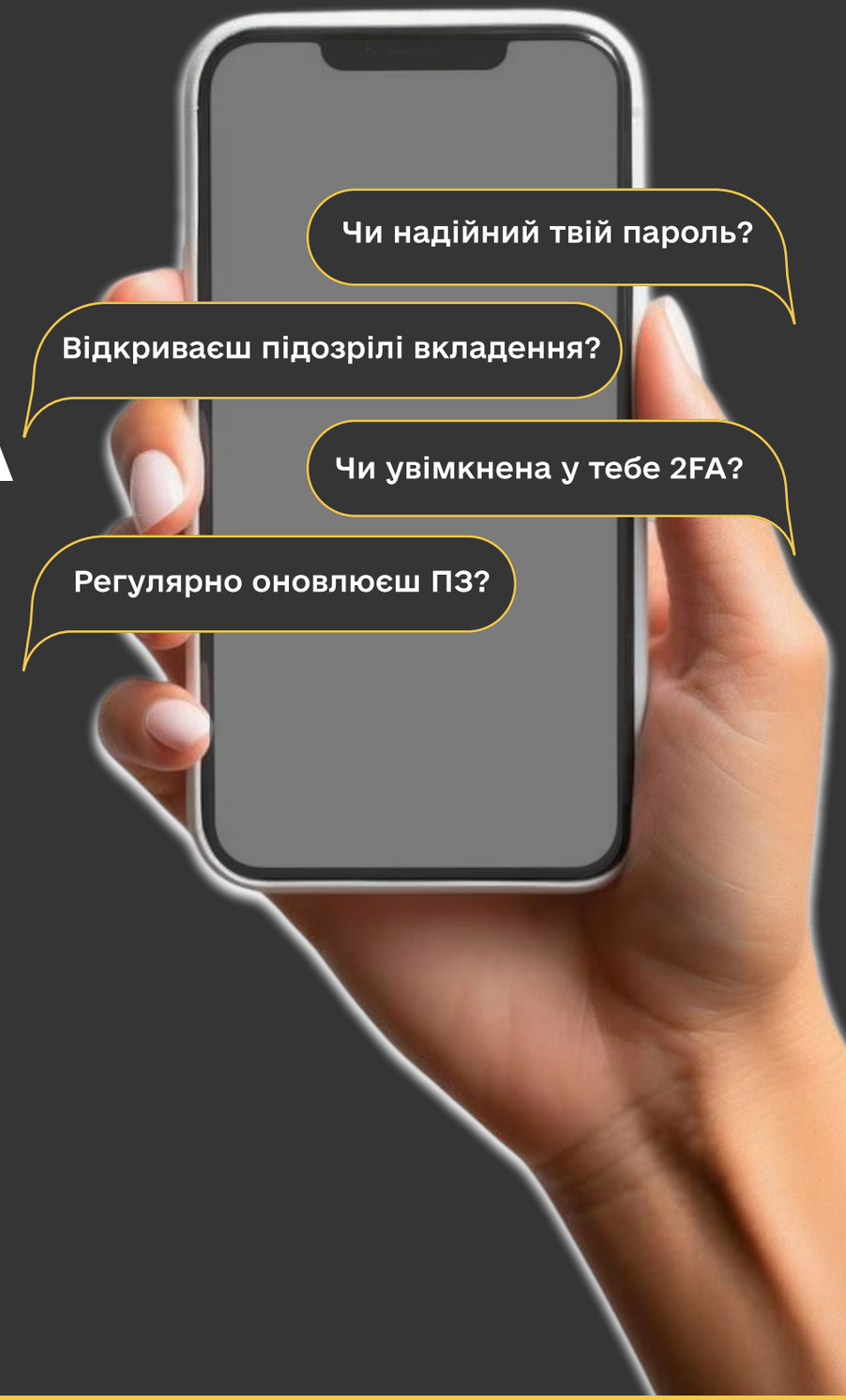
ОНЛАЙН-БЕЗПЕКА

кібергігієна сьогодні — цифрова безпека щодня



Запорізька обласна державна адміністрація

цифрова безбар'єрність

Управління з питань цифрового розвитку та інновацій, цифрових трансформацій і цифровізації

Кібергігієна — це сукупність правил, звичок і щоденних практик, які допомагають безпечно та відповідально користуватися цифровими технологіями, захищати особисті дані, пристрої та акаунти від кіберзагроз

Надійні паролі та 2FA

Перевірка достовірності та безпечності інформації в мережі

Захист даних

Оновлення ПЗ

Перевірка інформації та розпізнавання шахрайства

Пароль повинен:

бути достатньо довгим і складним

містити комбінацію великих і малих літер, цифр та спеціальних символів

бути унікальним для кожного сервісу: **один пароль — один обліковий запис**

не містити персональних даних (піб, дати народження), поширених слів і простих комбінацій символів

зберігатися в безпечному місці, а не у відкритому доступі, незахищених нотатках смартфона чи повідомленнях у месенджерах

1234567
password
qwerty
🙅‍♂️

dG@:CM450d&|
D|1w5g?!5E@U
👍

Двофакторна автентифікація – це використання одразу двох різних способів підтвердження входу

Додатковим фактором для перевірки може бути підтвердження:

- через код, надісланий у смс
- через дзвінок на мобільний
- через лист на e-mail
- через надсилання сповіщення – така можливість, наприклад, є для акаунтів Google
- через код, згенерований у Google Authenticator, Microsoft Authentificator)

Як встановити двофакторну автентифікацію:

1 Увійдіть у потрібний акаунт (наприклад, Facebook, Telegram, Google чи інший)

2 Зайдіть у розділ меню Налаштування, а потім Безпека

3 Оберіть пункт із налаштуваннями двофакторної автентифікації, якщо така функція є (може називатися також – двоетапна перевірка)

4 Виконайте всі необхідні дії за запропонованою інструкцією



Перевірка достовірності та безпечності інформації в мережі

1 довіряйте лише інформації з перевірених джерел, наприклад, вебсайти органів державної влади обов’язково мають закінчуватся на “gov.ua”

2 зверніть увагу на те, який протокол використовує сайт.
✅ **https** – надійний, забезпечує захищене з’єднання, конфіденційність інформації за допомогою шифрування
❌**http** – ненадійний

3 не використовуйте публічні wi-fi без паролю для входу в облікові записи, особливо для проведення банківських операцій. не під’єднуйтесь до невідомих пристроїв, які роздають інтернет

4 не оприлюднюйте в соцмережах та не надсилайте на вимогу незнайомців особисту інформацію: фото документів, телефонні номери, адресу, дані банківської картки тощо

5 не вводьте жодних особистих даних, якщо не впевнені у безпечності сайту

6 не переходьте за невідомими посиланнями, особливо, якщо вас спонукають зробити це «терміново»

7 не скануйте qr-коди з невідомих джерел

8 регулярно перевіряйте активні сеанси у своїх облікових записах

Будьте уважними до інформації, обережними з персональними даними та свідомими у кожній цифровій взаємодії 🤝

Оновлення програмного забезпечення (ПЗ)

1 програми для навчання чи розваг завантажуйте тільки з офіційних джерел (google play, app store)

2 своєчасно оновлюйте операційну систему та програми

3 перевіряйте дозволи, які запитують застосунки. обмежуйте доступ додатків до камери, мікрофона та геолокації.

4 видаляйте застосунки, якими не користуєтеся

Регулярне оновлення програмного забезпечення усуває виявлені вразливості, захищає пристрої від кіберзагроз і забезпечує їхню стабільну роботу. Не відкладайте встановлення оновлень — це важливий елемент кібергігієни 🤝

5 хвилин на власну кібербезпеку 🔐

1. перевірте паролі

переконайтеся, що паролі складні, унікальні для кожного сервісу та не містять особистої інформації

2. увімкніть 2fa

активуйте двофакторну автентифікацію для електронної пошти, соціальних мереж та інших облікових записів

3. перевірте оновлення

переконайтеся, що операційна система та застосунки мають актуальні оновлення

4. перегляньте активні сеанси

перевірте, з яких пристроїв виконано вхід до ваших облікових записів. завершіть невідомі сеанси

5. перевірте налаштування приватності

перегляньте, хто має доступ до вашої особистої інформації, геолокації, контактів і фотографій

Кібербезпека починається з простих звичок та відповідального ставлення до власних даних 🤝

Постійно вдосконалюйте цифрові знання та навички, щоб бути обізнаними щодо сучасних кіберзагроз і безпечно користуватися цифровими сервісами.

Навчатися та підвищувати рівень цифрової грамотності можна безкоштовно [на порталі «Дія.Освіта»]

