# 6 способів покращити вашу онлайн-безпеку

Ця порада ґрунтується на рекомендаціях Національного центру кібербезпеки.

Ви можете покращити свою кібербезпеку, здійснивши наступні шість дій:

Дія 1: Використовуйте надійний та унікальний пароль для своєї електронної пошти.

Дія 2: Створюйте надійні паролі, використовуючи 3 випадкові слова.

Дія 3: Зберігайте свої паролі у браузері.

Дія 4: Увімкніть двоетапну перевірку (2SV).

Дія 5: Оновіть свої пристрої.

Дія 6: Створюйте резервні копії даних.

## ДІЯ 1: Використовуйте надійний та унікальний пароль для своєї електронної пошти.

Якщо хакер проникне у вашу електронну пошту, він зможе:

- Скинути паролі інших облікових записів.
- Мати доступ до збереженої вами інформації про себе чи свій бізнес.

Ваш пароль електронної пошти повинен бути надійним і відрізнятися від усіх інших паролів. This will make it harder to crack or guess.

Використання трьох випадкових слів - хороший спосіб створити надійний, унікальний пароль, який ви пам'ятатимете.

Ви також повинні захистити інші важливі облікові записи, такі як банківські аккаути або соціальні мережі.

### А ви знали?

Якщо хакер отримає доступ до вашої електронної пошти, він може скинути паролі для інших облікових записів, використовуючи функцію "забув пароль".

### Як змінити пароль електронної пошти

Як змінити свій пароль у:

- Gmail.
- Yahoo!.
- Outlook.
- BT.
- AOL Mail.

Якщо ваш сервіс електронної пошти не вказаний у цьому списку, вам слід пошукати в Інтернеті поради вашого провайдера про те, як змінити пароль електронної пошти.

## Поради щодо паролів для індивідуальних підприємців та малого бізнесу

Якщо ви є власником бізнесу, ваші облікові записи можуть містити конфіденційну інформацію про ваших клієнтів, ваш бізнес або ваші фінанси.

Якщо ваші рахунки не захищені, ваш бізнес може зазнати більшого ризику кібер-атаки. Це може піддати ваш бізнес юридичному чи фінансовому ризику, а також ризику порушення Загального положення щодо захисту даних (GDPR).

Якщо у вашому підприємстві є співробітники, ви повинні переконатися, що вони не зберігають свої паролі поряд зі своїми пристроями, а також, що пристрої заблоковані або вимкнені, коли не використовуються.

Для отримання додаткової інформації див. посібник NCSC з малого бізнесу.

## ДІЯ 2: Створюйте надійні паролі, використовуючи три випадкові слова

Коли ви використовуєте різні паролі для важливих облікових записів, важко запам'ятати їх усі.

Хорошим способом створення надійних паролів є використання трьох випадкових слів.

Не використовуйте слова, які можна вгадати (наприклад, ім'я дитини). За потреби можна використовувати цифри та символи. Наприклад: “RedPantsTree4!”

Збереження паролів у браузері допоможе вам керувати ними.

### Перевірте свої знання щодо створення надійного пароля

Питання: Який із цих паролів не входить до топ-100 000 найненадійніших паролів?

- arsenal22
- 1v&upjw3nt
- p@55w0rd
- RedPantsTree
- Victoria!
- 2011977

### Відповідь Створення надійного пароля

Відповідь - RedPantsTree.

Хакери обмінюються в Інтернеті списками, що містять мільйони зламаних паролів.

3 випадкові слова - це більш простий спосіб створення нових паролів, які з більшою ймовірністю будуть унікальними для вас і з меншою ймовірністю будуть вгадані.

## ДІЯ 3: Зберігайте свої паролі у браузері

Зберегти пароль у браузері - це дозволить вашому веб-браузеру (наприклад, Chrome, Safari або Edge) запам'ятати пароль за вас.

Вони можуть допомогти вам:

- Переконайтись, що ви не втратили і не забули свої паролі.
- Захиститись від деяких кіберзлочинів, наприклад підроблених веб-сайтів.

Це безпечніше, ніж використання слабких паролів або використання одного пароля в декількох місцях.

Make sure you protect your saved passwords in case your device is lost or stolen.

### Як захистити збережені паролі

Той, хто отримає доступ до вашого пристрою, може використовувати збережені паролі для доступу до облікових записів.

Цей вид кіберзлочинів зустрічається набагато рідше, ніж віддалені атаки через Інтернет, коли паролі зламуються за допомогою програмного забезпечення.

Щоб переконатися, що ви захищені, ви повинні:

- Вимикайте або блокуйте пристрій, коли ви не користуєтеся.
- Використовуйте надійний пароль для захисту пристрою.
- Увімкніть двоетапну перевірку для всіх пристроїв та облікових записів.
- Увімкніть біометрію (Face ID або розпізнавання відбитків пальців), якщо пристрій підтримує цю функцію.

Також слід регулярно створювати резервні копії даних. Це допоможе вам відновити важливу інформацію у разі втрати або крадіжки пристрою.

### Як зберегти паролі у браузері

Дізнайтеся, як зберегти свої паролі в:

- Google Chrome.
- Microsoft Edge.
- Firefox.
- Safari.

## А ви знали?

Ви можете отримати доступ до збережених паролів з будь-якого пристрою, на якому ви увійшли до того ж браузера.

## Додати додатковий захист

Після того, як ви встановили надійні, окремі паролі (дії 1-3) для всіх своїх пристроїв та сервісів, ви можете зробити інші речі, щоб знизити ризик бути зламаним (дії 4-6).

## ДІЯ 4: Увімкніть двоетапну перевірку (2SV).

Двоетапна перевірка (2SV) допомагає запобігти проникненню хакерів у ваші облікові записи, навіть якщо вони мають пароль.

Деякі онлайн-банкінги використовують автоматично 2SV. Для цього він запитує додаткову інформацію, що підтверджує вашу особу, наприклад код, який відправляється на ваш телефон.

### Як увімкнути двоетапну перевірку (2SV)

Вам потрібно буде вручну включити 2SV для більшості ваших облікових записів. Не всі облікові записи пропонують 2SV. Онлайн-банкінг використовує 2SV автоматично.

2SV також відома як двофакторна автентифікація або багатофакторна автентифікація.

**Увімкніть 2SV для електронної пошти**

- Gmail.
- Yahoo.
- Outlook.
- AOL.

**Увімкніть 2SV для соціальних мереж**

- Instagram.
- Facebook .
- Twitter.
- LinkedIn.

## ДІЯ 5: Оновлюйте свої пристрої

Застаріле програмне забезпечення, програми та операційні системи мають слабкі місця. Це робить їх простішими для злому.

Компанії усувають недоліки, випускаючи поновлення. Коли ви оновлюєте пристрої та програмне забезпечення, це допомагає не допустити проникнення хакерів.

Увімкніть автоматичне оновлення для ваших пристроїв та програмного забезпечення, які пропонують. Це дозволить вам не запам'ятовувати щоразу.

Деякі пристрої та програмне забезпечення необхідно оновлювати вручну. Ви можете отримувати нагадування на ваш телефон або комп'ютер. Не ігноруйте ці нагадування. Оновлення допоможе забезпечити безпеку в Інтернеті.

### Як увімкнути автоматичне оновлення

Дізнайтеся, як увімкнути автоматичне оновлення для:

- Apple - Mac
- Apple - iPhone та iPad
- Microsoft Windows 10. - Пошук оновлень Windows 10
- Windows 7 більше не підтримується. Вам слід перейти на Windows 10
- Смартфони та планшети Android
- Android додатки

### Перевірте свої знання: Як компанії усувають слабкі місця у своєму програмному забезпеченні?

**Питання:** Як компанії усувають слабкі місця у своєму програмному забезпеченні?

- Бинт
- Патч
- Ремонт

**Відповідь:** Коли компанія знаходить слабке місце у своєму програмному забезпеченні, вона випускає «патч» для його усунення. Це допомагає зберегти вашу інформацію у безпеці.

## ДІЯ 6: Резервне копіювання даних

Резервне копіювання означає створення копії вашої інформації та збереження її на іншому пристрої або у хмарному сховищі (онлайн).

Регулярне резервне копіювання означає, що у вас завжди буде збережено останню версію вашої інформації. Це допоможе вам швидше відновити дані у разі їх втрати чи крадіжки.

Можна також увімкнути автоматичне резервне копіювання. Це дозволить регулярно зберігати вашу інформацію у хмарному сховищі без необхідності пам'ятати про це.

Якщо ви резервуєте копію інформації на USB-накопичувач або зовнішній жорсткий диск, від'єднуйте його від комп'ютера, коли резервне копіювання не виконується.

### А ви знали?

Перед оновленням пристрою слід створювати резервні копії даних.

Це пов'язано з тим, що оновлення можуть іноді видаляти або змінювати файли.

### Як увімкнути автоматичне резервне копіювання

Як увімкнути автоматичне резервне копіювання для:

- Apple – Mac.
- Apple - iPhone та iPad
- Android.
- Microsoft Windows 10 та Windows 8 OneDrive.

### Поради щодо резервного копіювання для індивідуальних підприємців та малого бізнесу

Резервне копіювання даних означає, що ваш бізнес зможе продовжувати працювати, якщо відбудеться кібер-інцидент.

Почніть з визначення даних, які є найбільш важливими для вашого бізнесу. Це може бути фінансова інформація, інформація про контракти, клієнтів або

постачальників. Переконайтеся, що резервне копіювання виконується регулярно.

Ви також повинні знати, як відновити резервну копію у разі втрати даних.

Для отримання додаткової інформації див. посібник NCSC з малого бізнесу.

## Більше порад про те, як залишатися в безпеці в Інтернеті

Фішинг: **Як повідомити NCSC?**

Дізнайтеся, як повідомити NCSC про потенційне фішингове повідомлення за допомогою служби Suspicious Email Reporting Service (SERS).

## Безпечні покупки в Інтернеті

Це керівництво допоможе вам уникнути шахрайських сайтів та безпечно придбати товари.