СИТУАЦІЙНИЙ ЦЕНТР ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СБУ

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ОБСЄ Організація з безпеки і співробітництва в Європі

НАЦІОНАЛЬНА РАДА УКРАЇНИ З ПИТАНЬ ТЕЛЕБАЧЕННЯ І РАДІОМОВЛЕННЯ

РАДА ВЕРХОВНА РАДА УКРАЇНИ

Комітет Верховної Ради України з питань свободи слова

ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ

«ПЕРСОНАЛЬНІ КОМП'ЮТЕРИ»

РЕКОМЕНДАЦІЇ ДЛЯ МЕДІА

ЧАСТИНА ІІ

2025

Базові рекомендації щодо підвищення рівня кібер-безпеки при використанні ПК з операційною системою Windows

1. Використовувати операційну систему **Windows 10/11**

2. Створити обліковий запис без прав адміністратора для щоденної роботи

3. Ввімкнути блокування екрана після 5 хвилин неактивності

4. Переконатись, що **Windows Update** увімкнено

5. Увімкнути **Microsoft Defender** або інше антивірусне програмне забезпечення

6. Увімкнути автоматичне сканування та захист у реальному часі

7. Увімкнути **Windows Firewall** (Брандмауер)

8. Вимкнути доступ до командного рядка: клавіша **Win+R** та вводимо **gpedit.msc**

(окрім Windows home)

GPO (gpedit.msc): User configuration > **Policies** > Administrative templates > **System** > Prevent Access to the command prompt > **Enabled**

9. Вимкнути доступ до **cmd**, **powershell**, **wscript**, **regedit GPO (gpedit.msc)**

User configuration > Policies > **Administrative templates** > System > **Prevent Access to the command prompt** > Enabled : cmd.exe, powershell.exe, regedit.exe, wscript.exe, wt.exe, WindowsTerminal.exe

10. Вимкнути виконання скриптів та сценаріїв **Powershell**

GPO (gpedit.msc): Computer Configuration > **Policies** > Administrative Templates > **Windows Components** > Windows PowerShell > **Turn on PowerShell** > Script Block > **Logging Enabled** > Turn on Script > **Execution Enabled**, Execution Policy: Allow only signed scripts

11. Заборонити використання гостьових облікових записів

GPO (gpedit.msc): Computer Configuration > **Policies** > Windows Settings > **Security**

Settings > Local Policies > **Security Options Accounts: Guest account status Disabled**

12. Заборонити автоматичне відкриття та запуск підключених носіїв даних

GPO (gpedit.msc): Computer Configuration > **Policies** > Administrative Templates > **Windows Components** > AutoPlay Policies > **Disallow Autoplay for non-volume devices** > Enabled > **Set the default behavior for AutoRun** > Enabled, Default AutoRun

Behavior: Do not execute any autorun commands > Turn off Autoplay Enabled, Turn off Autoplay on: All drives

13. Заборонити правити завдання в **Task Scheduler**

GPO (gpedit.msc): Administrative Templates > **Windows Components** > Task Scheduler > **Prohibit browse or GPO computer configuration/windows settings/security settings/file system C:** > WINDOWS > **system32** > taskschd.msc and C: > **Windows** > System32 > **Tasks** > deny permissions for users

14. Вимкнути макроси в **Office**

GPO (gpedit.msc): Computer or User Configuration > **Policies** > Administrative Templates > **Microsoft Office** > Security Settings > **Disable VBA for Office applications**

User configuration > **Policies** > Administrative templates > **Microsoft Word** > Word options > **Security** > Trust Centre > **Disable all macros with notification**

15. Увімкнути **BitLocker**

Панель керування > Система й безпека > **BitLocker Drive Encryption**

16. Вимкнути мікрофон, камеру та геолокацію, (**Параметри** > **Конфіденційність**)

Давати дозвіл на доступ до мікрофона, камери тільки програмам, яким це потрібно (**Zoom**, **Teams**, etc)

17. Постійно оновлювати Інтернет-браузери та програмне забезпечення

18. Не зберігати паролі в браузері

19. Встановити надійний пароль до свого облікового запису

20. Не запускати підозрілі файли (особливо **.exe**, **.bat**, **.scr**)

21. Регулярно перевіряти флеш-носії антивірусним ПЗ

22. Не переходити за підозрілими посиланнями

23. Активувати двофакторну автентифікацію (**2FA**) на всіх важливих акаунтах

24. Не використовувати однаковий пароль для кількох сайтів

25. Використовувати лише ліцензійні програмні продукти

Базові рекомендації щодо підвищення рівня кібербезпеки при використанні ПК з операційною системою MacOS

1. Шифрування диска (FileVault)

- увімкнути в **System Preferences > Security & Privacy > FileVault**
- захист паролем користувача
- перевірити, чи не використовується слабкий пароль облікового запису
- створити резервну копію ключа відновлення та зберігати її на офлайн-носії

1.1. Як зробити копію ключа відновлення на офлайн-носії:

- при ввімкненні **FileVault** macOS запропонує зберегти Recovery Key — виберіть **Create a recovery key and do not use my iCloud account**
- скопіюйте ключ вручну в менеджер паролів або текстовий файл
- заархівуйте файл з ключем (наприклад, у ZIP із паролем)
- збережіть його на зовнішній USB-накопичувач або зовнішній SSD/HDD, який не підключено постійно
- надійно зберігайте цей пристрій (наприклад у сейфі)

2. Secure Boot

За замовчуванням ввімкнений, але рекомендовано перевірити:

- перезавантажте Mac і натисніть та утримуйте **Power** (живлення), поки не з'явиться **Options >** Виберіть Options **> Continue** для входу в Recovery
- у верхньому меню оберіть **Utilities > Startup Security Utility**
- перевірте, що обрано **Full Security** (повна безпека)
- за потреби вимкніть дозвіл на зовнішнє завантаження (**External Boot: disallowed**)

3. Контроль доступів (TCC)

У **System Preferences > Security & Privacy**:

- обмежити доступ до мікрофона, камери, локації, файлової системи
- відключити зайві автоматизації (Automation) між додатками

4. Touch ID та пароль

- використовувати **Touch ID** + складний пароль (12+ символів)
- вимкнути автоматичний вхід: **System Preferences > Users & Groups > Login Options > Automatic login: Off** (потрібно натиснути замок внизу для змін)

- встановити вимогу пароля після сну або блокування: **System Preferences > Security & Privacy > General > Require password [5 секунд] after sleep or screen saver begins**

- увімкнути екранну заставку з вимогою пароля: **System Preferences > Desktop & Screen Saver > Screen Saver**, обрати заставку та активувати через кути екрана або таймер

- використовувати **Touch ID** + складний пароль (12+ символів)

- вимкнути автоматичний вхід

- встановити вимогу пароля через 5 секунд після сну або блокування

- увімкнути екранну заставку з вимогою пароля

5. Обмеження служб

- вимкнути **Remote Login: System Preferences > Sharing > Remote Login** — зняти галочку

- вимкнути **AirDrop: Finder > Go > AirDrop > Allow me to be discovered by: No One**

- вимкнути **Bluetooth: System Preferences > Bluetooth > Turn Bluetooth Off**, або через меню на панелі

- встановити правило: все, що не використовується регулярно — вимикається

6. Автозапуск і моніторинг

- перевірка автозапуску користувача: **System Preferences > Users & Groups > [Ваш користувач] > Login Items** — видалити зайві елементи

- перегляд системного автозапуску: **Terminal > launchctl list** — аналіз системних агентів/демонів

6.1. Рекомендовано використовувати утиліту **KnockKnock** для перегляду launch-агентів:

- завантажити з https://objective-see.org/products/knockknock.html

- надати привілеї повного доступу до диску: **System Settings > Privacy & Security > Full Disk Access** (якщо не буде ПЗ в списку, то додати через +)

- запустити ПЗ та вибрати **Start Scan** після чого очікувати до появи вікна з текстом **Scan Complete** (в ньому може бути вказано перелік файлів, які попередньо перевірені на сайті **VirusTotal** та на які можуть бути спрацювання антивірусного ПЗ). У разі якщо спрацювань по VirusTotal немає, перевірити категорію зліва по кожному запису на предмет присутності ПЗ, яке попередньо не встановлювалось або є підозрілим (має назву з рандомним іменем). Додатково перевірити на наявність легітимного підпису

- перевірити **System Extension** на предмет присутності ПЗ, яке не встановлювалось користувачем: **System Preferences > General > Login Items & Extensions**

7. Оновлення системи

- оновлення **ОС: System Settings > General > Software Update**

- оновлення ПЗ: **App Store > Updates**

- перевірити оновлення ПЗ, яке використовується окремо від стандартного з ОС (браузери, офісний пакет тощо)

8. Веб-браузер і розширення

У разі використання сторонніх браузерів (**Firefox**, **Brave** тощо) рекомендується мінімальний перелік розширень для використання (вони містять БД з трекерами, рекламою та іншим):

- **uBlock Origin** — блокування реклами та трекерів

- **HTTPS Everywhere** — примусовий перехід при відвідуванні веб-сайтів на захищений протокол HTTPS

За можливості не зберігати паролі в браузері. Вимикання функції зберігання:

- **Google Chrome: Settings > Autofill > Password Manager >** Вимкнути «Offer to save passwords» і «Auto Sign-in»

- **Firefox: Settings > Privacy & Security > Logins and Passwords >** Зняти галочки з «Ask to save logins» і «Autofill logins and passwords»

- **Brave: Settings > Autofill > Passwords >** Вимкнути «Offer to save passwords» і «Auto Sign-in»

- **Vivaldi: Settings > Privacy > Passwords >** Вимкнути «Offer to save passwords» та очистити збережені паролі

ОПЦІОНАЛЬНО увімкнути ізольований профіль/контейнер для чутливих сайтів (Firefox Containers):

- встановлення розширення «Firefox Multi-Account Containers» з **addons.mozilla.org**

- після встановлення з’явиться іконка в панелі інструментів Firefox. Натиснути її **>** створіть новий контейнер (наприклад: Banking, Email, Social)

- при відкритті вкладки в контейнері, всі **cookie**, логіни та локальні дані будуть ізольовані від інших вкладок

- контейнерні профілі зберігаються у вашому профілі Firefox: ~/**Library**/**Application Support**/**Firefox**/**Profiles**/[**профіль**]/**containers.json**

- для відновлення скопіюйте цей файл до нового профілю або зробіть резервну копію усієї папки профілю Firefox перед переустановленням браузера або системи

- використання **VPN**

9. **Шифрування резервних копій даних на Mac (опціонально)**

- використання зовнішнього диску для зберігання **Time Machine** (інкрементальні резервні копії). При створенні потрібно вибрати **Encrypt Backups**

- при виборі диску потрібно орієнтуватись на об'єм диску в Macbook

Наприклад, якщо використовується ssd об'ємом 256 ГБ, то зовнішній диск обираємо мінімум 512 ГБ, 512 ГБ > 1-2 ТБ, 1 ТБ > 2-4 ТБ

10. **Шифрування зовнішніх дисків/флеш носіїв**

- у разі вибору для шифрування стандартних можливостей **macOS** зазначений носій буде доступний лише на macOS. Для сумісності флеш-носія з Windows можна обрати **VeraCrypt** (наприклад, форматування в **exfat** з наступним шифруванням)

Як розпізнати фішинг у електронній пошті: практичні поради

Фішинг (англ. phishing, від fishing – рибальство) — вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів — логінів та паролей.

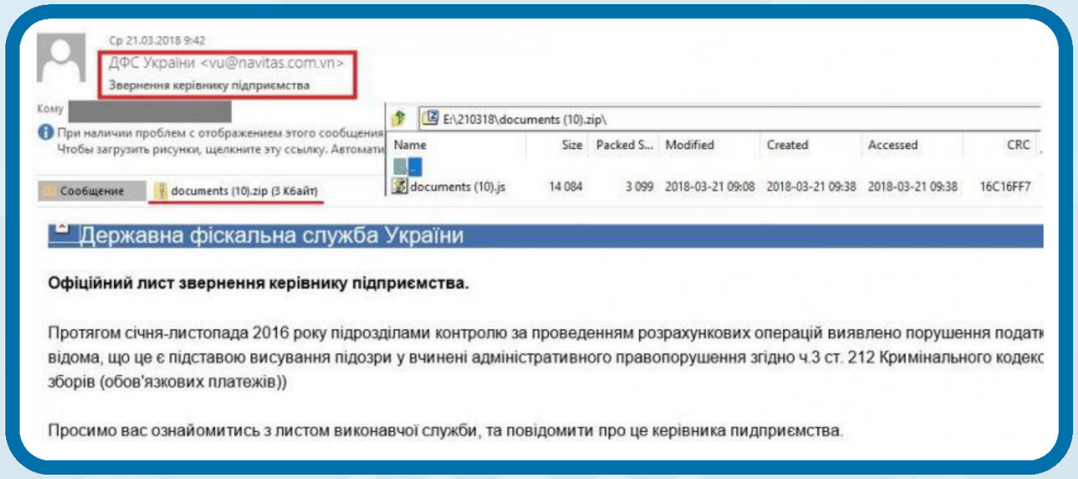
Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах від імені відомих організацій, наприклад, банків. У листі, зазвичай, міститься пряме посилання на сайт, який ззовні не відрізняється від справжнього. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами примусити його зазначити свій логін та пароль, який він використовує для отримання доступу до певного сайту. Отримання конфіденційної інформації користувача дає можливість шахраям використовувати облікові записи та банківські рахунки користувача в своїх цілях.

Ознаки фішингових листів

1. Адреса відправника

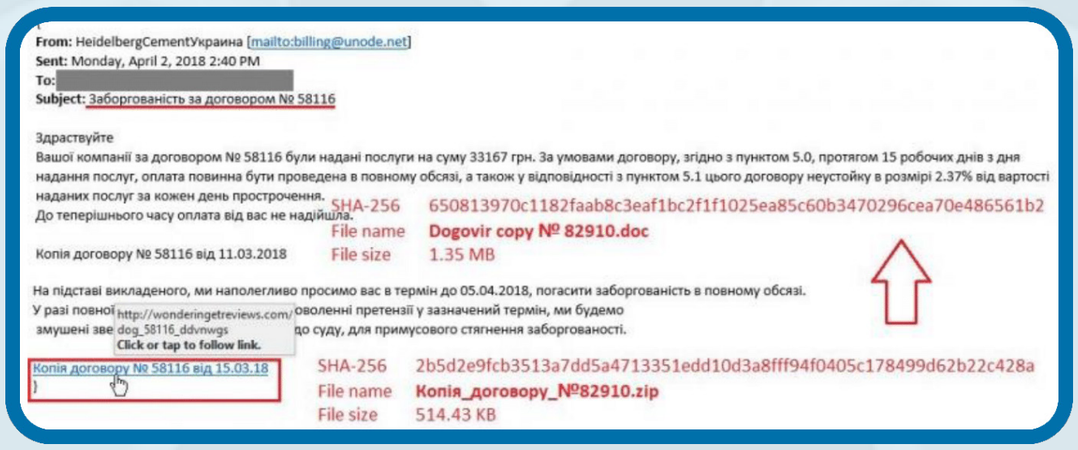
Електронна адреса, що відображається в полі «**Від:**» НЕ є гарантією відправки електронного листа через поштову систему від відповідного відправника.

За допомогою шкідливого програмного забезпечення шахраї можуть підмінити електронну адресу, яка відображається в будь-якому поштовому клієнті.



2. Екстрений характер повідомлення

З метою збільшення кількості успішних фішингових атак зловмисники намагаються надати повідомленням екстрений характер, окреслюючи ліміт часу, і викликати необдумані дії користувача.

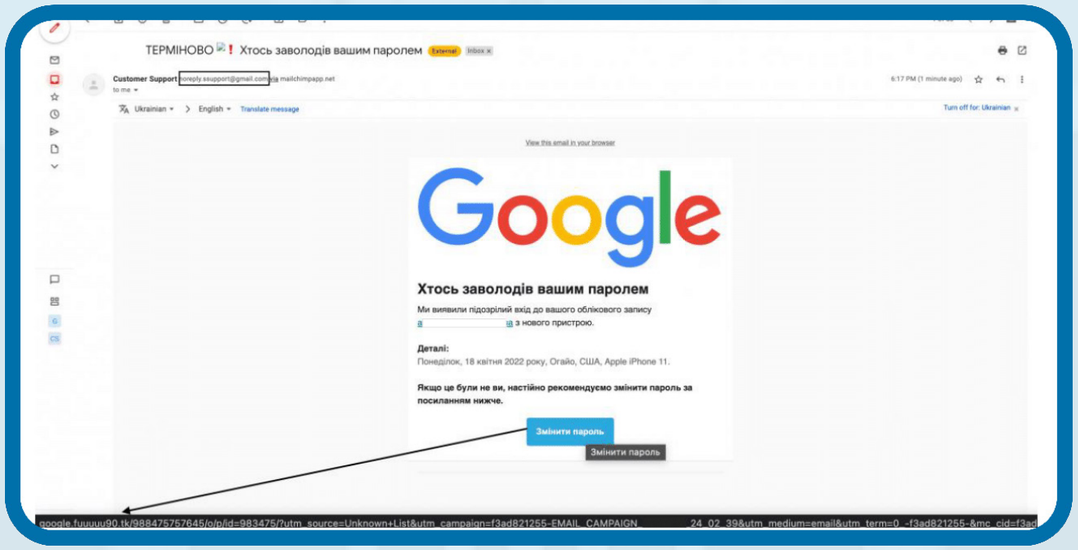


3. Помилки в темі листа

Як правило, в фішингових листах, в полі «**Тема:**», використовується різний регістр літер, набір літер та цифр, допускаються граматичні або друкарські помилки (наприклад **пОмиЛка**, **1нформац1я**) для уникнення фільтрів поштових програм.

4. Гіперпосилання на підроблені сайти

Посилання, зазначені в фішингових листах, ззовні схожі на офіційну вебадресу Компанії (наприклад, **Facebook**, **Google**) і перенаправляють користувачів на веб-сайти, які імітують зовнішній вигляд легітимного сайту Компанії.



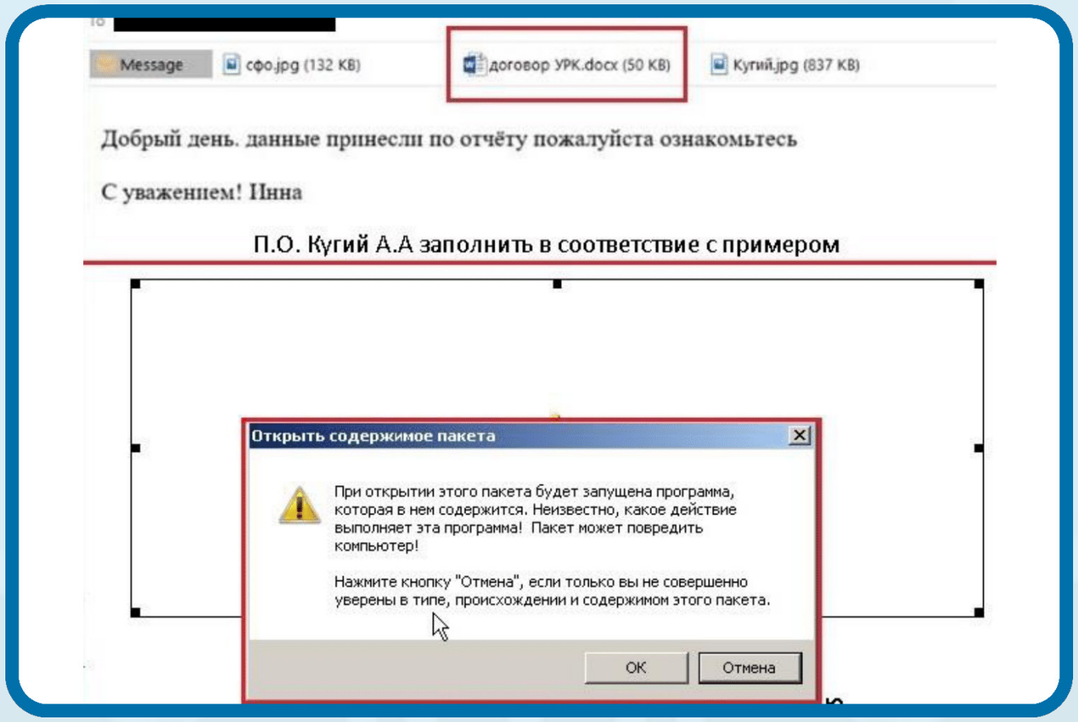
Більшість методів фішингу зводиться до маскування підроблених посилань на фішингові сайти під посилання реальних організацій. Шахраї часто використовують адресу з друкарськими помилками або субдомени.

В дійсності, адреса сайту (**URL**) складається з набору цифр та літер і вміст сайту є підробленим. Але частина інформації та некритичні посилання можуть бути оригінальними.

На зображенні справа представлено скріншот вебсайту, на якому попри фірмові логотипи і вказану назву, відображається адреса, яка не належить Netpeak.

5. Запити на виконання програм та увімкнення макросів

Якщо Ви відкрили документ або перейшли за посиланням і Вас просять або увімкнути макроси, або вимкнути режим захищеного перегляду, чи запустити зовнішню програму тощо — у жодному разі не робіть те, що від вас вимагають.



Як захиститися від фішингових атак?

1. Ніколи не надавайте логін, пароль та інші конфіденційні дані стороннім особам. Не відповідайте на листи з проханням вислати Вашу особисту або фінансову інформацію та не переходьте по вказаних посиланнях, оскільки всі листи з запитом конфіденційної інформації є шахрайськими.

2. Якщо Ви отримали сумнівний електронний лист від імені Компанії (наприклад, Вашого банку), повідомте про це Контакт-Центр відповідної Компанії або перешліть сумнівний лист з коментарями на відповідну електронну адресу Компанії.

3. Використовуйте останню версію браузера. Такі браузери як **Internet Explorer**, **FireFox**, **Google Chrome**, **Opera** систематично оновлюються і мають фільтр захисту від фішингу.

4. При передачі персональної інформації завжди перевіряйте та використовуйте шифроване з'єднання. При використанні безпечного з'єднання адреса сайту завжди розпочинається з «**https://**», а не з http://.

5. Для підтвердження автентичності сайту необхідно перевірити цифровий сертифікат безпеки шляхом натискання на символ безпечного з'єднання в Вашому браузері.

Рекомендації щодо захисту Wi-Fi мережі

Отримання несанкціонованого доступу до вашої Wi-Fi мережі може загрожувати такими проблемами як:

• **Збої в роботі роутера**. Завантаження відеоконтенту або онлайн-ігор сторонніми особами створює підвищене навантаження на мережу, через що Wi-Fi роутер зависає. В результаті ви не зможете в повній мірі скористатися швидкістю Інтернету.

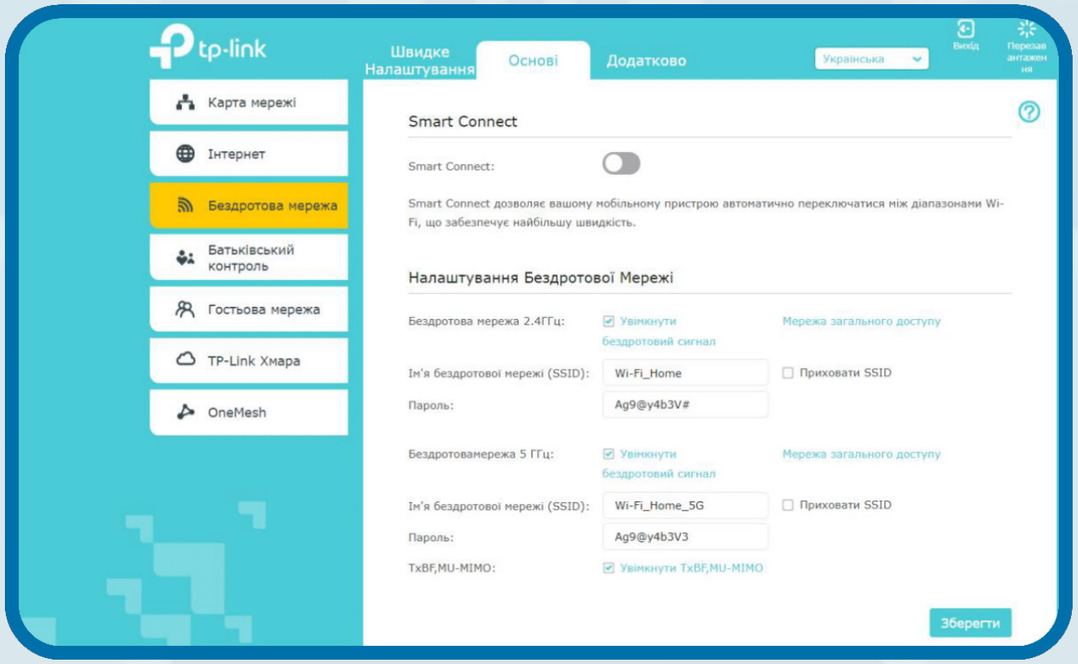
• **Доступ до приватної інформації**. Незапаролений Wi-Fi дає змогу отримати доступ до вашого браузера та особистих даних (листування, паролів до платіжних систем і відвідуваних сайтів, а також дій та покупок в Інтернеті).

• **Неправомірне використання вашого імені**. Не виключено, що підключення до вашого незахищеного Wi-Fi призведе до вчинення протиправних дій від вашого імені (завантаження забороненого контенту, відео або навіть виманювання грошей у ваших близьких і знайомих).

Щоб посилити безпеку мережі, можна вдатися до таких основних способів (на прикладі найбільш розповсюдженого виробника TP-Link):

Придумати надійний пароль

Чим складніший пароль, тим надійніший захист. В ідеалі він повинен складатися з великих та малих літер, цифр та спеціальних символів.



Щоб запаролити Wi-Fi мережу, потрібно зайти в налаштування роутера. Там знайти «**Бездротова мережа**», зайти у вкладку «**Безпека**», ввести новий пароль у відповідне поле та зберегти зміни. Також для зниження ризику зламу в подальшому не забувайте хоча б раз на 3 місяці оновлювати пароль.

Захистити доступ до маршрутизатора

Підключившись до вашої мережі, стороння особа може отримати доступ до налаштувань роутера і поміняти їх за бажанням. Щоб запобігти цьому, потрібно змінити стандартний логін та пароль для авторизації у налаштуваннях роутера.

1. Під'єднайтеся до роутера за допомогою Wi-Fi або кабелю.

2. В адресний рядок введіть **IP** пристрою (зазвичай він вказаний на наліпці).

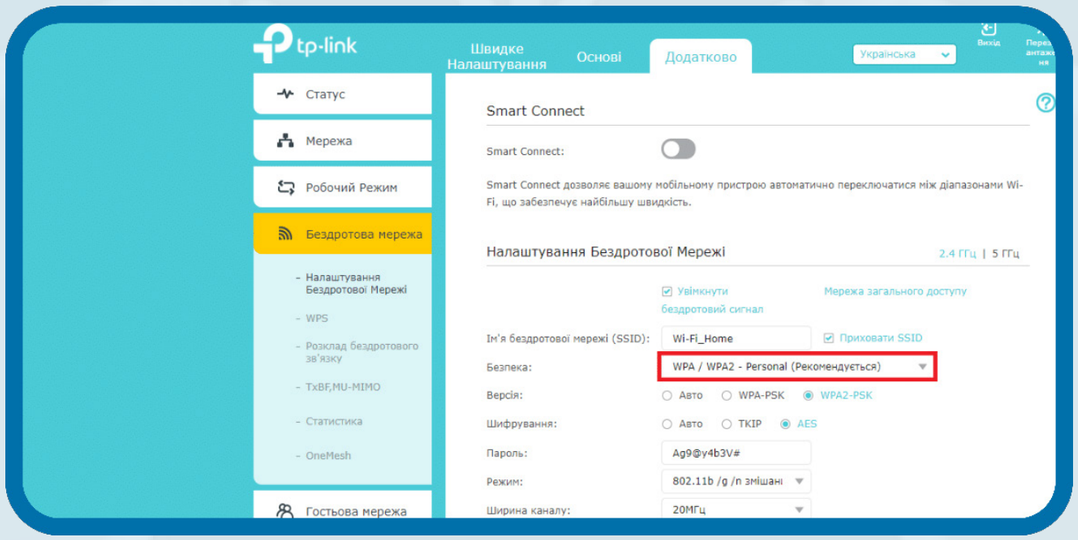
3. Впишіть логін і пароль від веб-інтерфейсу роутера (зазвичай це «**admin**») в обидва рядки.

4. В меню веб-інтерфейсу, знайдіть розділ «**Адміністрування**». Сюди введіть нові дані автентифікації та підтвердіть внесені зміни.

Встановити мережеве шифрування

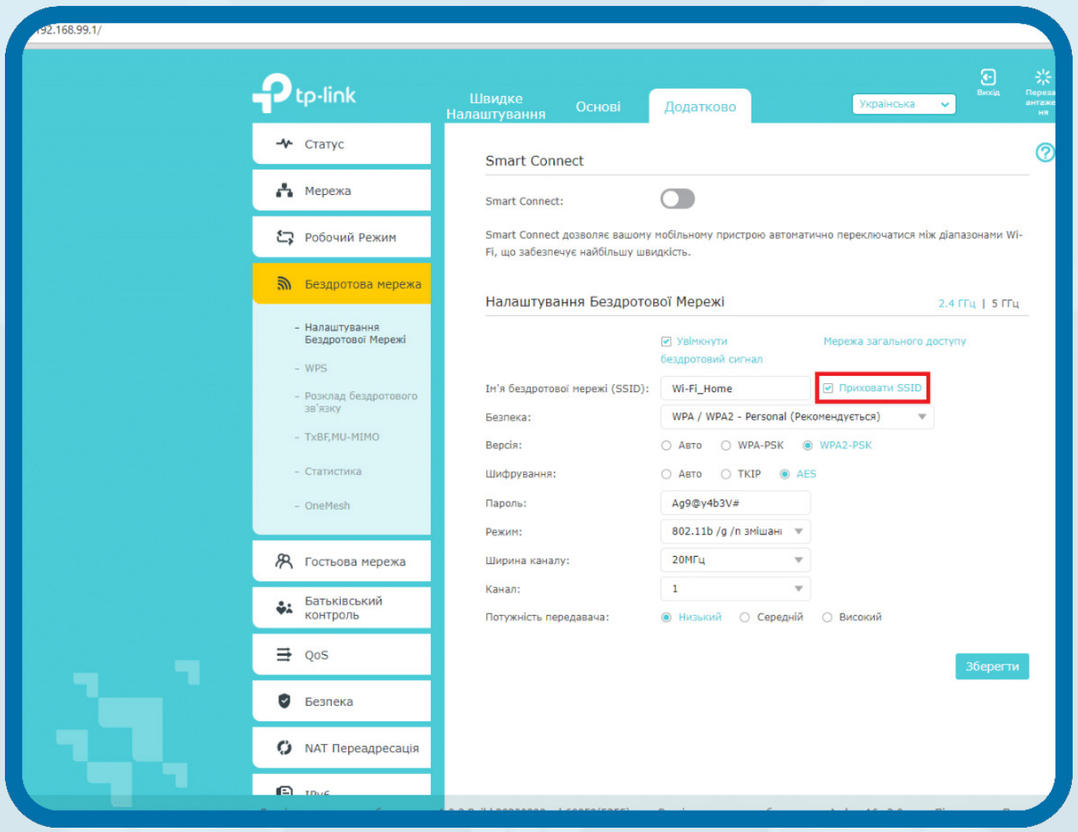
У розділі з опцією заміни пароля від Wi-Fi мережі є можливість вибрати той чи інший тип шифрування. Серед рекомендованих для використання:

- **WPA2/AES** - найпопулярніший на сьогодні варіант, який є простим і досить надійним.
- **WPA3** - цей метод автентифікації підтримують роутери з Wi-Fi 6 (802.11 ax), а також більшість моделей сучасних смартфонів та ноутбуків з Wi-Fi.



Приховати свою Wi-Fi мережу

Це ускладнить протиправним особам отримання доступу до роутера. Для цього в розділі «**Бездротова мережа**» потрібно поставити галочку навпроти пункту «**Приховати SSID**» або «**Приховати точку доступу**». Після цього необхідно зберегти зміни і перезавантажити роутер.



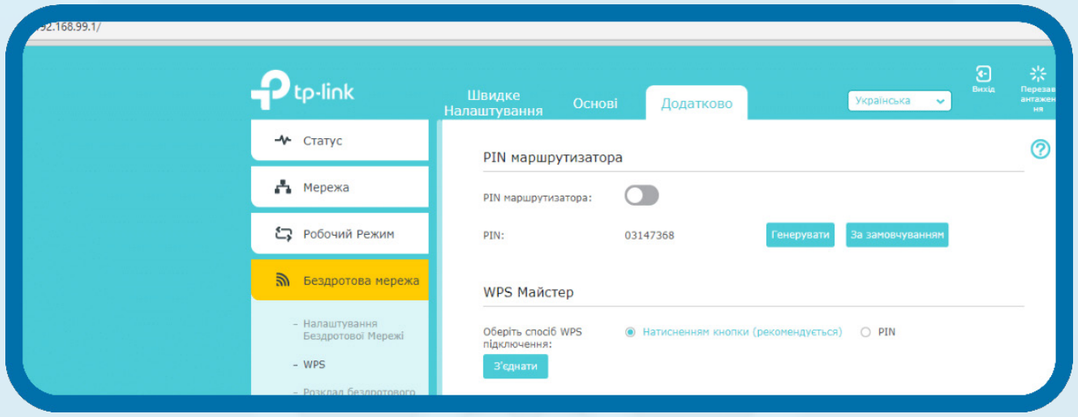
Для підключення до свого Wi-Fi буде потрібно:

1. Вибрати пункт «Інші мережі» на ПК або «Додати мережу» на смартфоні.

2. Ввести ім'я мережі та пароль.

Вимкнути WPS

За допомогою цієї зручної функції девайси можна підключати до Wi-Fi роутера без введення паролю. Але це робить бездротову мережу вразливою до небезпек. Щоб деактивувати **WPS**, достатньо зняти галочку з цього пункту в налаштуваннях маршрутизатора.



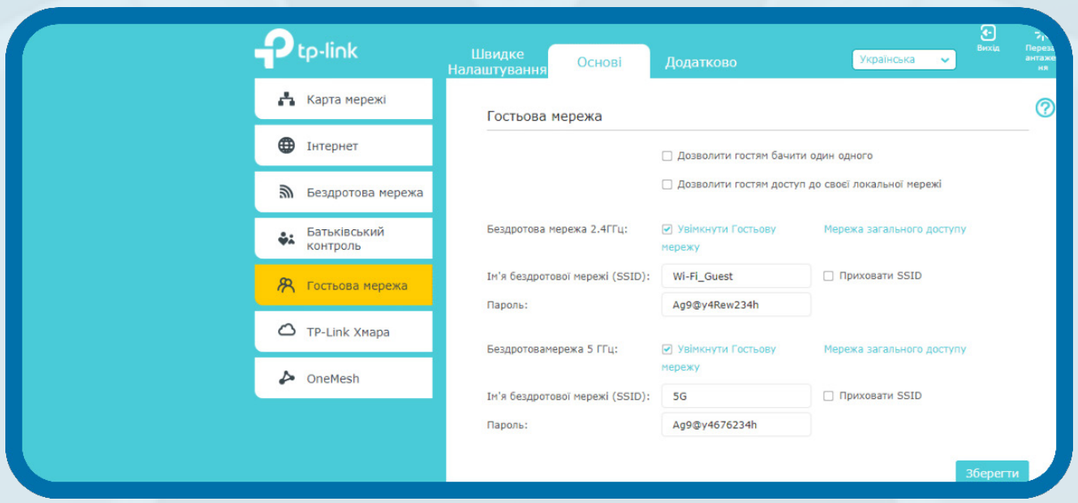
Крім вже перелічених, є й інші способи захистити домашній роутер від підключень сторонніх осіб:

Вимкнути віддалений доступ

Така опція дозволяє керувати роутером за допомогою зовнішнього сигналу. Зазвичай віддалений доступ потрібний провайдерам, щоб усунути проблеми з Інтернетом, не виїжджаючи до користувача. Але для безпеки Wi-Fi краще вимкнути цю опцію, зайшовши в налаштування в меню «Безпека».

Створити гостьову підмережу

У багатьох сучасних роутерів є можливість створювати **VLAN** — віртуальну гостьову мережу. Підключені до неї пристрої не отримують доступ до Вашої основної домашньої мережі, завдяки чому дані залишаються надійно захищеними.



Щоб увімкнути цю функцію, потрібно зайти в налаштування Wi-Fi мережі, встановити ім'я мережі для гостей та ввести пароль від неї.

Регулярно оновлювати прошивку

Для посилення захисту маршрутизатора та й в цілому більш коректної його роботи рекомендуємо дотримуватися наступних правил:

- На час оновлення підключайте роутер до комп'ютера виключно за допомогою дроту.
- Виберіть відповідну версію ПЗ. Перепишіть номер і серію маршрутизатора з наліпки і введіть ці дані на сайті виробника.
- У процесі прошивки від'єднайте роутер від зовнішньої мережі.
- Після завантаження потрібного файлу знайдіть в меню пункт «Оновлення», а потім виберіть свій файл і підтвердіть запуск процесу.

Обмежити радіус покриття

Сигнал від вашого Wi-Fi роутера можуть зловити не тільки в сусідній квартирі, але й у сусідньому будинку. Тож якщо у списку підключених до вашої мережі пристроїв ви помітили незнайомі, їх треба видалити. А щоб зробити бездротову мережу менш помітною, необхідно звузити зону покриття. Для цього потрібно перейти в налаштування маршрутизатора через веб-інтерфейс і знайти опції для зменшення радіусу покриття або зміни параметрів сигналу.

Зробити фільтрацію MAC-адрес

MAC-адреса — це унікальний ідентифікатор кожного пристрою. Більшість роутерів дозволяють створювати списки гаджетів: «білі» і «чорні». Для налаштування фільтра в меню є спеціальна опція.

Подивитися **MAC** клієнтського девайса можна у властивостях підключення на ПК або в розділі «Інформація про пристрій» на смартфоні. Кожен новий гаджет, який потрібно буде внести до списку, доведеться прописувати в налаштуваннях.

Використовувати брандмауер і VPN

Для запобігання атакам можна скористатися спеціальними засобами захисту. Наприклад, такими як брандмауер, фаєрвол, **DoS** та інші. Якщо в роутері наявні такі функції, їх навіть не треба вмикати, адже вони активовані стандартно.

Якщо маршрутизатор підтримує **VPN**, ви також можете активувати цю функцію. Вона дозволяє створити зашифрований тунель для захисту як роутера, так і всіх підключених до мережі пристроїв.

Для повідомлення щодо протиправних дій у сфері інформаційної безпеки (Департамент кібербезпеки СБУ):

- E-mail: **cyber_security@dis.gov.ua**

Для невідкладного інформування про кіберінциденти та кібератаки (Ситуаційний центр забезпечення кібербезпеки СБУ)

- E-mail: **incident@dis.gov.ua**