Ситуація 1

Персональні дані 20 млн користувачів безкоштовних VPN-сервісів опинились у відкритому доступі через недбалість розробників цих сервісів. Про це [повідомив](https://www.hackread.com/vpn-firm-zero-logs-policy-leaks-20-million-user-logs/) портал HackRead.

Експерти з кібербезпеки виявили незахищений сервер з базою обсягом 1,2 тб з даними з різних VPN-додатків. Зокрема, на сервері знаходяться дані додатків UFO VPN, Fast VPN, Free VPN, Super VPN, Flash VPN, Secure VPN і Rabbit VPN.

В базах знайшли електронні адреси, зашифровані паролі, IP- і домашні адреси, дані про моделі смартфонів та ідентифікатори пристроїв користувачів.

У частини додатків більше 1 млн завантажень в Google Play і AppStore, а користувацький рейтинг – вище 4,5.

«Такий витік шокує і демонструє повне нехтування правилами безпеки, яке ставить під загрозу користувачів», – заявили дослідники.

Фахівці відзначають, що інтернет-користувачі повинні уникати безкоштовних послуг VPN, щоб не стати жертвами подібних витоків. Справа в тому, що безкоштовні VPN-рішення забезпечують мінімальний рівень анонімності і захищеності мережевого трафіку.

Експерти наголошують, що втрачені дані користувача можуть в подальшому використовуватися для спаму, фішингових розсилок або шантажу клієнтів VPN-сервісів.

Ситуація 2

Кіберполіція виявила та затримала зловмисників, які вимагали гроші за відновлення доступу до акаунтів у соціальних мережах. За допомогою шкідливого програмного забезпечення зловмисники отримували незаконний доступ до електронних поштових скриньок, які були пов'язані з акаунтами жертв..

На електронні поштові скриньки власників акаунтів соцмережі Instagram здійснювалася розсилка листів, які були інфіковані шкідливим програмним забезпеченням. Всі ці листи були замасковані під нібито офіційні повідомлення служби підтримки соціальної мережі. У подальшому, отримавши доступ, зловмисники вносили зміни до реєстраційних даних, чим блокували доступ справжнім власникам. Під час повернення доступу вони вимагали від 10 до 30 тис. гривень у криптовалюті.

Зазвичай у ролі жертв обирали сторінки, кількість підписників яких була більшою за 15 тис користувачів (сторінки Інтернет-магазинів, відомих людей тощо).

Так зловмисники заволоділи сторінками в соціальних мережах більш як тисячі громадян України та іноземців.

Співробітники поліції спільно зі столичною прокуратурою провели санкціоновані обшуки за місцем проживання одного з учасників групи. Під час обшуку поліцейські вилучили комп'ютерну техніку, її вже спрямовано на проведення всіх необхідних експертиз.

За виявленими фактами розпочато кримінальне провадження за двома статтями Кримінального кодексу України. Зловмисникам загрожує до восьми років позбавлення волі.

Ситуація 3

За [інформацією](https://ssu.gov.ua/novyny/na-zhytomyrshchyni-sbu-blokuvala-prodazh-danykh-iz-baz-derzhavnoi-podatkovoi-sluzhby) спецслужби, головний державний ревізор-інспектор за винагороду пропонував надати відомості про доходи фізичних та юридичних осіб регіону з автоматизованої інформаційної системи «податковий блок». Замовниками таких послуг були місцеві приватні підприємці, яких цікавила інформація про конкурентів та потенційних клієнтів. Вартість інформації залежала від обсягів і носія даних.

Правоохоронці задокументували кілька фактів збуту податківцем персональної інформації. Його затримали у Бердичеві під час отримання оплати від чергового клієнта.

Під час обшуків за місцем роботи та проживання податківця правоохоронці вилучили комп’ютерну техніку та накопичувачі з інформацією з обмеженим доступом, які він планував продати.

Якщо вину податківця доведе суд, то йому загрожує до двох років ув’язнення або штраф.

Ситуація 4

Група хакерів заявила про злам польської компанії-розробника ігор CD Projekt RED та отримання доступу до вихідного коду її ігор Cyberpunk 2077 та «Відьмак 3». Про це сама компанія CD Projekt RED [повідомила](https://twitter.com/CDPROJEKTRED/status/1359048125403590660) у Twitter, де і опублікувала лист від хакерів.

Зловмисники заявляють, що отримали доступ до вихідного коду ігор «Відьмак 3», Cyberpunk 2077, «Гвинт». Також хакери стверджують, що їм вдалось викрасти внутрішню документацію компанії пов'язаної з бухгалтерським обліком та адмініструванням, даних про угоди з інвесторами, документів з юридичного відділу, відділу HR тощо.

Окрім цього у листі злочинці зазначили, що зашифрували сервери CD Projekt RED, хоча й розуміють, що компанія може відновити дані з резервних копій.

Хакери дали компанії 48 годин для виконання своїх вимог, хоча чого саме хочуть зловмисники у листі не вказано. В разі невиконання вимог вони погрожують продати код або опублікувати його онлайн, а також передати корпоративну інформацію журналістам.

Ситуація 5

Хакер на замовлення здійснював злам платних програм для технічних спеціалістів. Чоловік вносив зміни до програмного коду, щоб обійти ліцензію та зробити програми безкоштовними. Замовниками були переважно іноземні громадяни.

Під час обшуків у нього вилучили комп’ютерну техніку. Відкрито кримінальне провадження ч. 2 ст. 361 ККУ (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку).

Ситуація 6

У Нідерландах журналіст взяв участь у секретній конференції міністрів оборони країн Європейського союзу завдяки залишеним у мережі даними для входу в цю відеозустріч. Про це повідомляє [BBC](https://www.bbc.com/news/world-europe-55027641).

Даніель Верлан з RTL Nieuws підключився до відеоконференції після того, як міністр оборони Нідерландів випадково розмістила в Twitter деякі дані для входу в систему. Журналіст долучився до конференції саме у розпал обговорень і помахав міністрам рукою. Відповідаючи на запитання високого представника ЄС Жозепа Борреля, Верлаан представився голландським журналістом.

Після цього Боррель наголосив, що підключення до закритої відеоконференції є порушенням закону і таку витівку журналіста можуть визнати кримінальним злочином. Журналіст з посмішкою перепросив за те, що перервав важливу нараду, і залишив онлайн-зустріч.

 «Ви знаєте, що потрапили на секретну конференцію?» Ви знаєте, що це кримінальний злочин, а вам краще відключитися, перш ніж приїде поліція», — запитав журналіста Верховний комісар ЄС із зовнішньої політики Жозеп Боррель. Журналіст вибачився і покинув відеоконференцію.

Зазначається, що журналісту вдалося отримати доступ після того, як міністр оборони Нідерландів Анк Бійлевельд опублікувала в Твіттері фотографію, яка містила адресу для входу та частину PIN-коду. Після декількох спроб журналісту вдалося підібрати відсутню цифру PIN-коду й увійти у відеоконференцію.

Ситуація 7

Шахраї заволоділи будівлею в центрі Києва, надіславши державному нотаріусу лист з комп’ютерним вірусом, повідомила кіберполіція.

За [інформацією](https://cyberpolice.gov.ua/news/u-kyyevi-kiberpolicziya-vykryla-fakt-shaxrajskogo-zavolodinnya-neruxomistyu-za-dopomogy-kompyuternogo-virusu-3654/) правоохоронців, зловмисники, використовуючи шкідливе програмне забезпечення, отримали віддалений доступ до комп’ютера державного нотаріуса. Після цього вони внесли зміни до реєстру прав власності на нерухомість.

Таким чином, шахраї заволоділи будівлею площею 250 квадратних метрів у центрі Києва.

Поліцейські встановили замовника, на прохання якого зловмисники надіслали державному нотаріусу електронний лист з вірусом. У нього вилучили комп’ютерну техніку з доказами причетності до несанкціонованого втручання у роботу комп’ютера державного нотаріуса. Проти нього відкрили кримінальне провадження за статтею «Шахрайство» Кримінального кодексу України. У разі доведення вини, замовнику таких послуг загрожує до восьми років в’язниці.

Зазначимо, що вірус в електронних листах спрацює у разі, якщо отримувач відкриє вкладення чи посилання, яке у ньому знаходиться. Відтак кіберполіція не повідомила, чи нестиме відповідальність державний нотаріус, який запустив вірус на своєму комп’ютері.

Ситуація 8

Троє 19-річних мешканців Дніпропетровщини ошукали на понад мільйон гривень громадян країн Європи та Америки шляхом створення фейкових сайтів на яких постраждалі залишали свої банківські дані. Про це [розповіли](https://mvs.gov.ua/uk/press-center/news/kiberpoliciya-dnipropetrovshhini-vikrila-zlovmisnikiv-u-privlasnenni-grosei-inozemciv-za-dopomogoyu-fisingu) у кіберполіції України

У відомстві зазначили, що такий вид шахрайства називається фішинг. Зловмисники створили десяток фішингових інтернет-майданчиків оголошень, де користувачі вводили дані своїх кредиток. Сайти повністю копіювали дизайн іноземних інтернет-майданчиків оголошень.

Зібрані дані карток зловмисники підв’язували до системи безконтактної оплати на телефонах. З рахунків потерпілих фігуранти розраховувалися за покупки у магазинах побутової техніки.

Наразі поліцейські встановлюють, кого саме ошукали українці. Попередня сума збитків сягає понад мільйон гривень.

У помешканнях фігурантів правоохоронці провели обшуки та вилучили мобільні телефони, комп’ютерну техніку та банківські картки. Усе направили на експертизу.

Кримінальне провадження відкрили за ч. 2 ст. 200 (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків). Санкція статті передбачає до 170 тис. гривень штрафу.

Ситуація 9

Група хакерів заявила про злам польської компанії-розробника ігор CD Projekt RED та отримання доступу до вихідного коду її ігор Cyberpunk 2077 та «Відьмак 3». Про це сама компанія CD Projekt RED [повідомила](https://twitter.com/CDPROJEKTRED/status/1359048125403590660) у Twitter, де і опублікувала лист від хакерів.

Зловмисники заявляють, що отримали доступ до вихідного коду ігор «Відьмак 3», Cyberpunk 2077, «Гвинт». Також хакери стверджують, що їм вдалось викрасти внутрішню документацію компанії пов'язаної з бухгалтерським обліком та адмініструванням, даних про угоди з інвесторами, документів з юридичного відділу, відділу HR тощо.

Окрім цього у листі злочинці зазначили, що зашифрували сервери CD Projekt RED, хоча й розуміють, що компанія може відновити дані з резервних копій.

Хакери дали компанії 48 годин для виконання своїх вимог, хоча чого саме хочуть зловмисники у листі не вказано. В разі невиконання вимог вони погрожують продати код або опублікувати його онлайн, а також передати корпоративну інформацію журналістам.