**У Кіберполіції назвали 6 схем, як шахраї можуть виманювати гроші онлайн**

З початку повномасштабної війни кіберполіція викрила майже 500 людей, причетних до [онлайн-шахрайства](https://www.pravda.com.ua/news/2022/06/12/7352025/).

Зловмисники можуть просити гроші нібито на ЗСУ або виманювати ваші дані карток, обіцяючи фінансову допомогу, [повідомляє](https://t.me/mvs_ukraine/14030) Міністерство внутрішніх справ.

Про злочинні схеми та кібератаки обов’язково потрібно повідомляти до [**Кіберполіції**](https://ticket.cyberpolice.gov.ua/) та Урядової команди реагування на компʼютерні надзвичайні події **CERT-UA**.

*"Це важливо робити, щоб фахівці блокували шахрайські схеми та кібератаки в інтернеті й притягали винних до відповідальності"*, – кажуть правоохоронці.

У Кіберполіції, Держспецзв’язку і Національному банку України також [пояснили](https://t.me/mvs_ukraine/14030?single), як розпізнати шахраїв і вберегтися від них.

**Читайте також:**[**Які файли та сайти НЕ можна відкривати? 4 правила кібербезпеки**](https://life.pravda.com.ua/society/2022/03/21/247905/)

**Як захиститись від шахраїв онлайн у різних випадках?**

|  |
| --- |
| https://life.pravda.com.ua/images/doc/b/2/b2b14ed-depositphotos-oogleb-cyber-crime-security-fraud-ukraine.jpg |
| *Фото: ooGleb/*[*Depositphotos*](https://ua.depositphotos.com/) |

**Схема 1:**

Знайома людина просить позичити грошей в особистому повідомленні в месенджері соціальної мережі. Це може бути хтось, із ким ви давно не спілкуєтесь, але є ризик, що сторінку людини зламали шахраї.

**Що робити:**

**✅**зв'язатися з людиною через інший канал (телефоном, поштою, іншим месенджером) і запитати про повідомлення.

Якщо людина не надсилала повідомлення:

**✅**розповісти, що її акаунт зламали;

**✅**порадити змінити пароль до месенджера та увімкнути двофакторну аутентифікацію;

**✅**попросити повідомити про інцидент Кіберполіцію та CERT-UA.

**Схема 2:**

Вам може надійти повідомлення в месенджері або пост у соцмережах про надання фінансової допомоги, яку може отримати будь-хто.

Гроші пропонують нібито від імені державних, міжнародних установ або банків.

Повідомлення зазвичай містить посилання на чат-бот або сайт, де нібито можна дізнатись додаткову інформацію.

**Як діяти:**

**✅**потрібно отримувати інформацію, особливо з приводу фінансових виплат, лише з офіційних джерел;

❌ не переходити за сумнівними посиланнями;

❌ не повідомляти конфіденційної інформації стороннім (дані картки, логін та паролі до онлайн банкінгу тощо);

**✅**якщо ж особисту (персональну) інформацію розголошено, потрібно звернутись до банку та заблокувати картку;

**✅**якщо підозрюєте шахрайство – негайно повідомляйте правоохоронців.

**Схема 3:**

Повідомлення про евакуаційний рейс за умови передплати.

**Що робити:**

**✅**перевіряти інформацію про евакуаційні рейси, гуманітарні коридори необхідно тільки на офіційних ресурсах;

**✅**обирати післяплату перевезень;

**✅**якщо ви постраждали від шахрайства, заповніть форму на [сайті кіберполіції](https://ticket.cyberpolice.gov.ua/).

**Читайте також:**[**Безпека у месенджерах: як захиститись від ворога онлайн?**](https://life.pravda.com.ua/society/2022/02/28/247602/)

**Схема 4:**

Зловмисники можуть "продавати" в інтернеті товари, яких насправді не існує, за передплатою.

**Як діяти:**

**✅**купуйте товари та сплачуйте кошти лише на перевірених сайтах;

**✅**у разі сумнівів, надайте перевагу післяплаті;

**✅**для онлайн-шопінгу відкрийте віртуальну картку і переказуйте на неї лише суму, необхідну для оплати;

❌ нікому не повідомляйте термін дії картки, CVV та PIN-код;

❌ при купівлі на платформі оголошень обговорюйте деталі угоди тільки в чаті цієї платформи – НЕ переходьте у сторонні месенджери;

**✅**перевіряйте правильність назви необхідного сайту: один непомітний символ на панелі адреси може означати, що ви потрапили на фішинговий ресурс.

**Схема 5:**

Псевдопокупець може запитати реквізити картки для оплати за ваш товар на дошці оголошень і називати час здійснення переказу.

У цей час напарник зловмисника під виглядом працівника служби безпеки банку може зателефонувати вам і сказати, що для зарахування грошей необхідно "активувати платіжну картку".

Він диктує реквізити підконтрольних рахунків, видаючи їх за коди активації картки.

**Як діяти:**

❌ не повідомляйте стороннім даних картки або даних, що можуть бути використані для підтвердження платежів;

❌ не виконуйте жодних операцій з "верифікації" карти;

**✅**у разі сумнівів – телефонуйте до банку за телефоном, вказаним на звороті картки, і уточніть інформацію.

**Схема 6:**

Розсилання повідомлень начебто від офіційних установ про збір коштів на ЗСУ.

**Що робити:**

**✅**переказуйте гроші лише через офіційні фонди, благодійні організації або людям, яких ви знаете особисто і яким довіряєте;

❌ не переходьте за сумнівними посиланнями;

❌ не вказуйте на сторонніх ресурсах даних вашої банківської картки.

**Якщо ви постраждали від злочину в інтернеті, заповніть форму на**[**сайті кіберполіції**](https://ticket.cyberpolice.gov.ua/)**, наголошують у МВС.**

|  |  |
| --- | --- |
|  |  |

[**СУСПІЛЬСТВО**](https://life.pravda.com.ua/society/2023/09/11/256471/)

[В Україні стане більше повністю придатних до військової служби: чи забиратимуть у військо з ВІЛ та туберкульозом](https://life.pravda.com.ua/society/2023/09/11/256471/)

[**Яна Осадча**](https://life.pravda.com.ua/society/2023/09/11/256471/)

[**ПОДОРОЖІ**](https://life.pravda.com.ua/travel/2023/09/10/256452/)

[Гори, полонини, водоспади та мінеральні води: куди поїхати в Карпати восени](https://life.pravda.com.ua/travel/2023/09/10/256452/)

**Анастасія КоропецькаКУЛЬТУРА**