# РОЗ'ЯСНЕННЯ З

# ОКРЕМИХ ПИТАНЬ

# ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

# Інструкція для населення що до захисту від шахрайства?

* не повідомляти особисту інформацію особам, які телефонують та представляються брокерами чи працівниками банку;
* за жодних умов не розкривати реквізити своїх банківських карток; - отримуйте інформацію лише з перевірених джерел КМУ, МОЗ, МВС; - здійснюйте купівлі на перевірених сайтах, а також за допомогою накладеного платежу;
* перевіряйте дані приводця через антишахрайський майданичик в загальному користуванні «STOPFRAUD», який дозволяє перевірити громадянам абонентський номер та банківську картку на причетність до вчинення шахрайських дій;
* перевіряйте назви сайтів на відповідність офіційним вебсайтам;
* встановлюйте ліцензійне програмне забезпечення, яке може попереджати про шахрайські веб ресурси, за можливості користуйтеся застосунками Apple/Google Pay, не вводьте на сайтах реквізити банківських платіжних карток.

# Шахрайства в сфері фінансових розрахунків, а саме при роботі з

**казначейськими програмами та інше**

Для захисту акаунтів у банківських застосунках використовуйте складні паролі, які містять літери верхнього та нижнього регістру, цифри та символи. Не встановлюйте однаковий пароль для декількох акаунтів. Налаштуйте двофакторну аутентифікацію всюди, де є така можливість. Тоді для входу до акаунту, крім логіну та паролю, потрібно ввести додатковий кодпідтвердження, причому пароль рекомендується змінювати не рідше ніж раз на місяць, а у двохфакторну ідентифікацію робити персоналізовано під кожного співробітника.

Не переходьте за сумнівними посиланнями, адже за ними може ховатися фішинговий ресурс. Ніколи не вводьте конфіденційні дані на підозрілих сайтах.

Подбайте про захист фінансового номера. Забороніть віддалений перевипуск SIM-карти у мобільного оператора або перейдіть на контрактне обслуговування.

Не допускайте наявності віддаленого доступу до персонального комп’ютера та встановлення програмного забезпечення призначеного для

фінансових розрахунків, постійно оновлюйте антивірусне програмне забезпечення.

# За побігання шахрайства та стратегії протидій

Робота щодо протидії онлайн-шахрайствам ведеться у режимі 24/7, розроблено рішення з метою блокування підозрілих вебресурсів у соціальних мережах та маркетплейсах, спільно з ЄМА блокуються банківські рахунки якими користуються шахраї, розроблено та впроваджено систему автоматичного блокування фішингових вебресурсів, забезпечується документування організованих груп та злочинних організацій. Хочу зазначити, що ні один шахрай не зникне з поля зору кіберполіції та у будь-якому випадку буде притягнений до відповідальності.

# Чи існують методи виявлення кібершахрая, якщо відомо номер його

**мобільного?**

В більшості випадків на кожний епізод злочинної діяльності шахраї використовують новий абонентський номер телефону який до цього ніде не використовувався, тому ідентифікувати особу в даному випадку стає складніше. Але все одно за допомогою програмно-технічного забезпечення, у тісній взаємодії із операторами телекомунікаційних послуг ці особи ідентифікуються та в подальшому у відношенні їх проводиться комплекс необхідних слідчорозшукових дій з метою притягнення до відповідальності шахраїв. Якщо перевірити мобільний номер телефону бажає цивільна особа, то для цього можливо використати застосунок Get Contact та Trucaller, або ввести номер телефону до пошуковика Google, оскільки користувачі мережі Інтернет могли обговорювати діяльність такого номера мобільного телефону.

# Які реальні методи притягнення до відовідальності кібершахраїв +

**статистика?**

З початку 2022 року працівниками ДКП в рамках кримінальних проваджень проведено **1783** обшуків, повідомлено про підозру **747** особі, **444** проваджень направлено до суду з обвинувальним актом. Задокументовано діяльність **16** організованих груп та злочинних організацій. **210** особам застосовано запобіжний захід у вигляді тримання під вартою.

## Приклади

30.01.2023 за матеріалами ДКП направлено до суду кримінальне провадження від 27.05.2022 з обвинувальним актом за ч.5 ст.27, ч.3 ст.28, ч.3 ст.190, ч.4 ст.190, ч.2 ст.200, ч.5 ст. 361 КК України відносно учасників організованої злочинної групи у складі 3-х осіб встановлено, що учасники ОГ в період відбування покарання у виді позбавлення волі в установі виконання покарань – державній установі «вінницька виправна колонія (№86)», шахрайським шляхом, використовуючи електронно-обчислювальну техніку, видаючи себе за працівників служби безпеки банків, попередньо отримавши від потерпілих конфіденційну інформацію щодо належних їм банківських рахунків, відкритих в ат кб «приватбанк», здійснили несанкціоноване втручання до облікового запису потерпілих, в автоматизованій системі дистанційного банківського обслуговування «приват24», що призвело до підробки, витоку та блокування інформації, яка обробляється у вище вказаній системі та в подальшому, шахрайським шляхом, використовуючи електронно-обчислювальну техніку, заволоділи коштами на загальну суму 1 млн. 202 тис. грн.

20.05.2023 за матеріалами ДКП повідомлено про підозру за ч.2 ст.255, ч.4 ст.28, ч.4 ст.190 КК України відносно ЗО у складі 5 осіб. Фігуранти з використанням електронно-обчислювальної техніки, спеціалізувались на розроблені фішингових-повідомлень, які імітували офіційні урядові та банківські веб-сайти України, пропонуючи громадянам України та особам, які постраждали внаслідок військових дій на території України отримання грошової допомоги від Президента України, ООН, «UNICEF» та інші. Від протиправної діяльності злочинної організації постраждало близько 1500 осіб, яким було завдано шкоди на загальну суму близько 4 млн. 600 тис. грн.

07.06.2023 за матеріалами ДКП повідомлено про підозру 3 фігурантам за ч. 1 ст. 209, ч. 3 ст. 190, ч. 5 ст. 361, ч. 2 ст. 361-1 КК України, які у складі ОГ у глобальній мережі Інтернет організували діяльність шахрайських інвестиційних проектів та створили фішингові Telegram-боти, що за своїм візуальним оздобленням сході на енергетичні компанії, з метою викрадення акаунтів користувачів у месенджері «Telegram» та подальшого використання облікових записів користувачів у спам-розсилці і рекламуванні псевдо інвестиційних шахрайських проектів, спрямованих на заволодіння грошовими коштами

громадян. Усього внаслідок несанкціонованого втручання в аккаунти постраждало близько 15 тисяч людей, а від шахрайських дій – близько 3 тисяч.

**Протидія фішінгу аккаунтів в соціальних мережах та месенджерах** *Аферисти поширюють фейкову інформацію про соціальні виплати, створюючи сторінки-клони державних організацій, керівництва держави, представників ООН, Червоного Хреста, благодійних фондів, банків тощо. Для реалізації злочину здебільшого використовують фішинг.*

Громадянам пропонують ввести персональні дані та номер банківської картки нібито для зарахування грошей. Однак відомості, введені на таких ресурсах, автоматично стають відомі зловмисникам. Маючи дані банківських карток громадян, вони привласнюють гроші з рахунків.

## Кіберполіція закликає громадян бути пильними та радить:

* отримувати інформацію, особливо з приводу фінансових виплат, лише з офіційних джерел;
* не переходити за сумнівними посиланнями;
* не повідомляти конфіденційну інформацію, зокрема дані банківських карток, стороннім;
* у разі підозри шахрайських дій - негайно повідомляти правоохоронним органам.
* Встановити додаткові ступені захисту у фінансових застосунках онлайн- банкінгу.

# Як відрізнити шахрайський лист від звичайного?

## Прохання підтвердити ваші особисті дані

Якщо ви не очікували отримання такого листа, але він раптом прийшов на вашу електронну скриньку, то це сигнал того, що лист може бути фальшивим.

## Адреса відправника не виглядає справжньою

Часто трапляється так, що фішинг-лист надходить з адреси, яка лише видається справжньою. Злочинці прагнуть обманути одержувачів, включивши назву реальної компанії в електронний адрес пошти відправника.

## Велика кількість граматичних помилок в тексті листа

Прочитайте електронну пошту та перевірте наявність орфографічних та граматичних помилок, а також дивних фраз. Електронні листи від офіційних компаній вичерпно перевіряються на наявність орфографічних, граматичних та інших помилок.

## Наявність підозрілих файлів, прикріплених до листа

Це досить сильна ознака фішингового листа, якщо ви не очікували та не запрошували отримати те чи інше вкладання. Вкладення може містити зловмисну URL-адресу, що призводить до встановлення вірусу чи зловмисного програмного забезпечення на вашому комп’ютері чи мережі.

## Наявність прикріплених до листа архівів

Наявність прикріплених до листа архівів може свідчити про те, що лист містить у собі заархівовану версію шкідливого програмного забезпечення, яке у свою чергу може викрадати конфіденційну інформацію та призводити до шахрайських дій відносно жертви.

**Ваші поради, як ма ксимально донести цю важливу інформацію до людей** *Якщо ви стикнулись із шахрайськими діями зверніться негайно до найближчого правоохоронного органу або залиште соє звернення на офіційному сайті Кіберполіції за посиланням https://ticket.cyberpolice.gov.ua/*

У своєму звернені до поліції надайте усю вичерпну інформацію стосовно вчинених проти вас протиправних дій. Скріншоти листування, чеки, квитанції про сплату коштів, ресурс на якому відбулось шахрайство, контактні дані особи яка вчинила шахрайство.

Додатково необхідно проводити загальнонаціональні роз’яснювальні кампанії як не стати жертвою шахраїв із залученням засобів масової інформації, волонтерів, громадських організацій, тощо.

## Для безпечного використання соцмереж радимо:

* не нехтувати двофакторною автентифікацією – це найкращий захист для Інтернет-акаунтів;
* використовувати складний пароль, різний для кожної соцмережі;
* не заходити до акаунтів з чужих пристроїв;
* ніколи не пересилати приватні фото або фотокопії документів: у разі зламу – ці дані опиняться у зловмисників;
* не переходити за сумнівними посиланнями;
* для онлайн-шопінгу використовувати перевірені ресурси та надавати перевагу післяплаті.

Громадянам також варто пам’ятати, що представники соцмережі ніколи не писатимуть в особисті повідомлення, а лише на пошту, вказану при реєстрації.