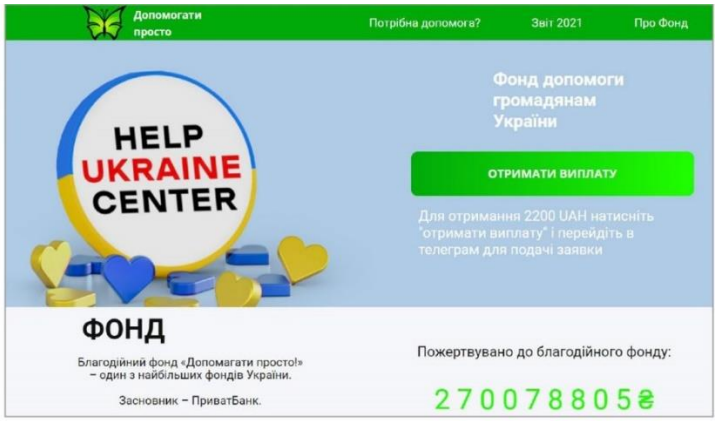
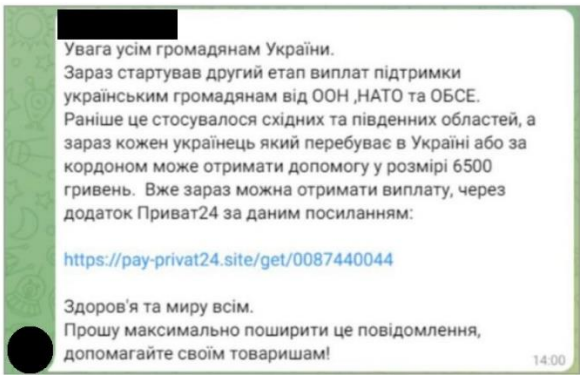
1. Грошова допомога.

В розповсюджених месенджерах та соцмережах шахраї під виглядом міжнародних організацій, соціальної платформи єДопомога, порталу державних послуг Дія, відомих українських брендів тощо пропонують громадянам, що постраждали від війни, отримати грошову допомогу.

Сценарії шахрайства з грошовою допомогою:

- Для отримання допомоги потрібно перейти за наданим посиланням, обрати банк та увійти у свій онлайн-банкінг. Насправді посилання веде на фішинговий сайт, що імітує обраний онлайн-банкінг, тому після введення облікових даних вони попадають до шахраїв, які, отримавши доступ до банківських рахунків жертви, знімають все до копійки та ще отримують на її ім’я онлайн-кредити.





- Для отримання виплати потрібно перейти за посиланням в чат-бот у Телеграмі, що імітує банківський чат-бот, де у жертви шахрайства випитують реквізити платіжної картки, облікові записи до онлайн-банкінгу, банківські SMS-паролі та ПІН-код. Результат той самий – жертву обдирають до нитки.
- Для отримання коштів потрібно сплатити державне мито. Але замість обіцяних грошей у жертви виманюють не лише гроші за сплату державного мита, але й реквізити платіжної картки. На цьому шахраї, зрозуміло, не зупиняються – жертву позбавляють грошей, що зберігаються на її картковому рахунку.
- Під приводом роздачі великих грошей від імені відомих українських компаній жертві пропонують пройти нескладне опитування, потім надіслати посилання на сайт своїм друзям, після чого заповнити форму з персональними даними і, нарешті, сплатити комісію.
  Але замість обіцяних грошей, в залежності від жадібності та креативності шахраїв, жертву підписують на сторонні сервіси з періодичним списанням грошей із «засвіченої» картки, виманюють реквізити платіжної картки або облікові записи до

онлайн-банкінгу. А викрадені у жертви персональні данні продаються оптом на чорному ринку та згодом використовуються проти неї в інших шахрайських схемах.

Поради, що працюють:

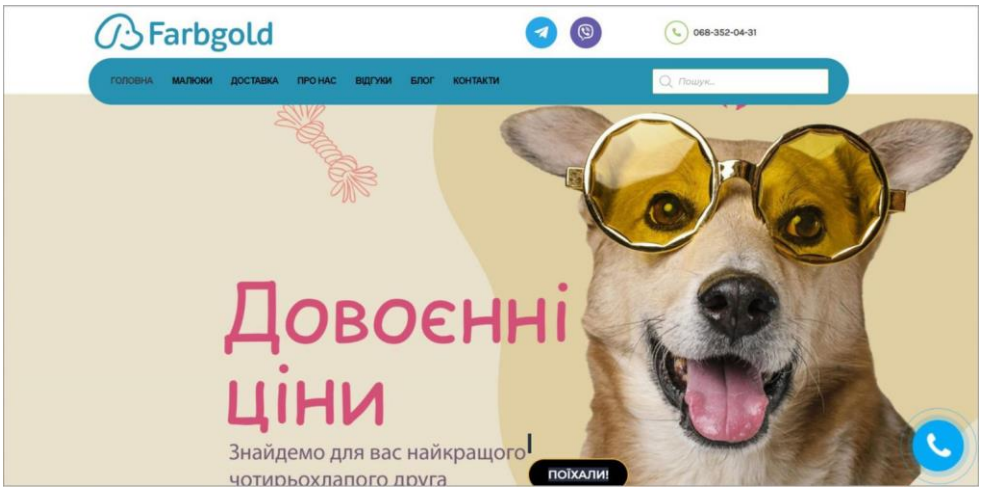
- Усі онлайн-послуги, що стосуються виплат від держави, міжнародних організацій можна отримати лише на порталі та в застосунку Дія, який потрібно завантажити лише з офіційного порталу Дія. Про зарахування коштів можуть повідомляти лише Дія та банк push-сповіщенням, у якому міститься лише текст, — жодних посилань. До того ж кошти зараховуються на картку автоматично, і ви можете одразу перевірити баланс у своєму онлайн-банкінгу.
- Якщо хтось вам пропонує отримати грошову допомогу через чат-бот, — це шахрайська схема! Якщо для отримання допомоги потрібно сплатити державне мито — це також шахрайська схема, оскільки під час отримання допомоги державне мито не сплачується.
- Офіційну інформацію про грошову допомогу від держави та міжнародних організацій шукайте на державному сайті groshi.edopomoga.gov.ua
- Будьте уважними до деталей під час введення своїх персональних даних, паролів, карткових реквізитів. Завжди звертайте увагу на доменне ім'я та зону сайту. Використовуйте для перевірки посилань та сайтів функціонал CheckMyLink або VirusTotal, який за лічені секунди безкоштовно перевірить сайт на шахрайство та віруси.

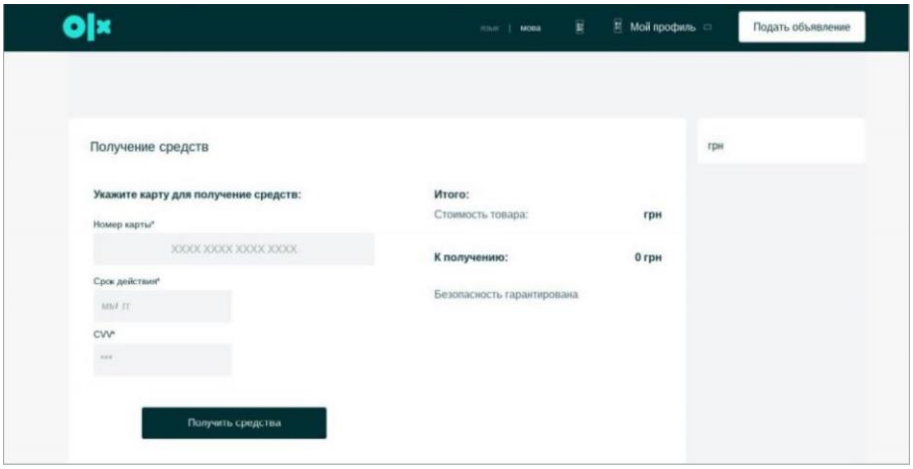
2. Інтернет-торгівля

Користуючись підвищеним попитом населення на товари, пов'язанні з військовою тематикою, нестачею електроенергії та товари повсякденного попиту за нижчими цінами, шахраї виманюють у громадян грошові кошти, карткові реквізити та облікові записи онлайн-банкінгу.

Сценарії шахрайства з Інтернет-торгівлею:

- Шахраї створюють шахрайські Інтернет-крамниці, вимагаючи попереднє внесення оплати за неіснуючі товари.
  Вдаючи з себе продавця на торговому онлайн-майданчику або дошці оголошень, шахрай виманює у покупця передоплату або, пропонуючи безпечну сплату за товар, стимулює перейти за фішинговим посиланням, та виманює реквізити платіжної картки або логін та пароль до онлайн-банкінгу.





Вдаючи з себе покупця на торговому онлайн-майданчику або дошці оголошень, шахрай стимулює продавця перейти за фішинговим посиланням, щоб отримати неіснуючу передоплату, ввівши всі реквізити платіжної картки.

Поради, що працюють:

- OLX багато зробив, щоб захистити своїх користувачів від різноманітних шахрайських схем, що постійно з'являються в Інтернет навколо цієї популярної дошки оголошень. Та самому користувачу теж потрібно дотримуватися простих і логічних правил. OLX-сайт один – OLX.UA
- Звертайте увагу на адресу (OLX має вигляд olx.ua, а мобільна версія сайту – m.olx.ua). Решта: olxposhta.com, olx.cx, 0lx.in.ua тощо – шахрайські сайти-клони. Лише на OLX! Не переходьте у месенджери!
- Оговорюйте деталі угод лише в особистому кабінеті OLX! Не переходьте у месенджери (Viber, Skype, Telegram, WhatsApp тощо) – там вас OLX вже не захистить.
- Усі угоди з «OLX.Доставка» лише на OLX.UA
  Оформлюйте угоди з «OLX.Доставка» лише на OLX.UA – в особистому кабінеті (вкладка «OLX.Доставка»).
- Довіряйте лише офіційним сайтам. Перш ніж ввести в будь-яку форму дані своєї платіжної картки або паролі до онлайн-банкінгу — перевірте сайт через функціонал CheckMyLink або VirusTotal, який за лічені секунди безкоштовно перевірить сайт на шахрайство та віруси.
- Платіть після отримання товару — замовляйте товари з попереднім внесенням оплати лише у перевірених та відомих Інтернет-магазинів.
- Великі знижки — одна з ознак шахрайських інтернет-крамниць та «лотів-приманок», розміщених шахраями на сайтах безкоштовних оголошень.
- Користуючись послугами торгових онлайн-майданчиків або дошок оголошень, не йдіть у месенджери, листуйтесь лише в чаті сервісу.
- Лише номер картки! — Пам'ятайте, для отримання будь-якого переказу на вашу картку достатньо надати покупцеві (відправнику грошей) лише її номер.

3. Телефонне шахрайство

Телефонні шахраї телефонують з підроблених номерів, використовуючи для цього спеціальні сервіси IP-телефонії з можливістю підміни номера, називаючи себе працівником банку, мобільного оператора або поліцейським, що розслідує шахрайські дзвінки, або розсилають відповідні SMS-повідомлення та повідомлення у месенджерах, мотивуючи жертву перетелефонувати, та виманюють у співрозмовника карткові реквізити, спонукають встановити програму для віддаленого доступу або переказати гроші на свій рахунок.

Розповсюджені сценарії телефонних атак:

- Шахрай, назвавшись банківським співробітником, залякує жертву повідомленням про спроби злому її банківського рахунку або підозрілі операції.
  Мета: під час розмови отримати у співрозмовника його карткові реквізити та банківські SMS-коди; змусити жертву переказати гроші на «безпечний рахунок» або прив'язати картку до телефонного номера шахрая.

- Шахрай, назвавшись банківським співробітником, під приводом підвищення заходів безпеки вмовляє жертву встановити на телефон програму віддаленого доступу.
  Мета: віддалено отримати доступ до мобільного банкінгу на пристрої жертви і дистанційно виконувати дії від її імені (наприклад, переказати гроші на будь-який рахунок).
- Шахрай, назвавшись банківським співробітником, виманює у жертви її кодове слово та персональну інформацію, необхідну для віддаленої ідентифікації в банку.
  Мета: використовуючи отриману від жертви інформацію, зателефонувати до банку та, назвавшись клієнтом, отримати доступ до банківського рахунку клієнта.
- Шахрай, назвавшись співробітником мобільного оператора, намагається виманити у жертви SMS-код, надісланий їй мобільним оператором.
  Мета: викрасти SIM-картку жертви, а разом з нею викрасти і її онлайн-банкінг, щоб здійснювати будь-які фінансові операції, користуючись банківським рахунком жертви, як своїм.

Поради, що працюють:

Три речі, які вам ніколи не запропонує зробити дійсний спів-робітник банку або мобільного оператора:

1. Надати CW-код безпеки зі звороту вашої картки, ПІН-код та облікові записи до онлайн-банкінгу.
2. Надати банківські SMS-коди та коди, отримані від мобільного оператора.
3. Встановити на телефон або ноутбук програму для віддаленого доступу (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin).

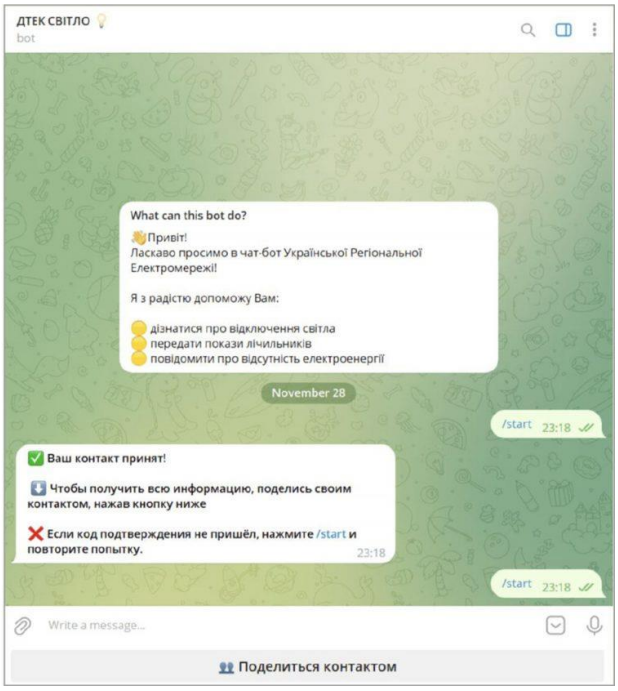
- Якщо співрозмовник представився співробітником банку, мобільного оператора, правоохоронних органів, регулятора, ніколи не повідомляйте йому трьохзначний CW-код безпеки зі звороту вашої картки, кодове слово, банківські SMS-коди та коди, отримані від мобільного оператора. Лише почули подібне прохання — перервіть розмову і повідомте вашбанк за номером, вказаним на звороті вашої картки.
- Пам'ятайте, у разі шахрайської операцій банк блокує рух коштів на картці, і сам клієнт телефонує для розблокування, називаючи кодове слово та надаючи персональну інформацію для віддаленої ідентифікації; зворотна ситуація — це шахрайство.

4. Викрадення акаунтів у соцмережах та месенджерах.

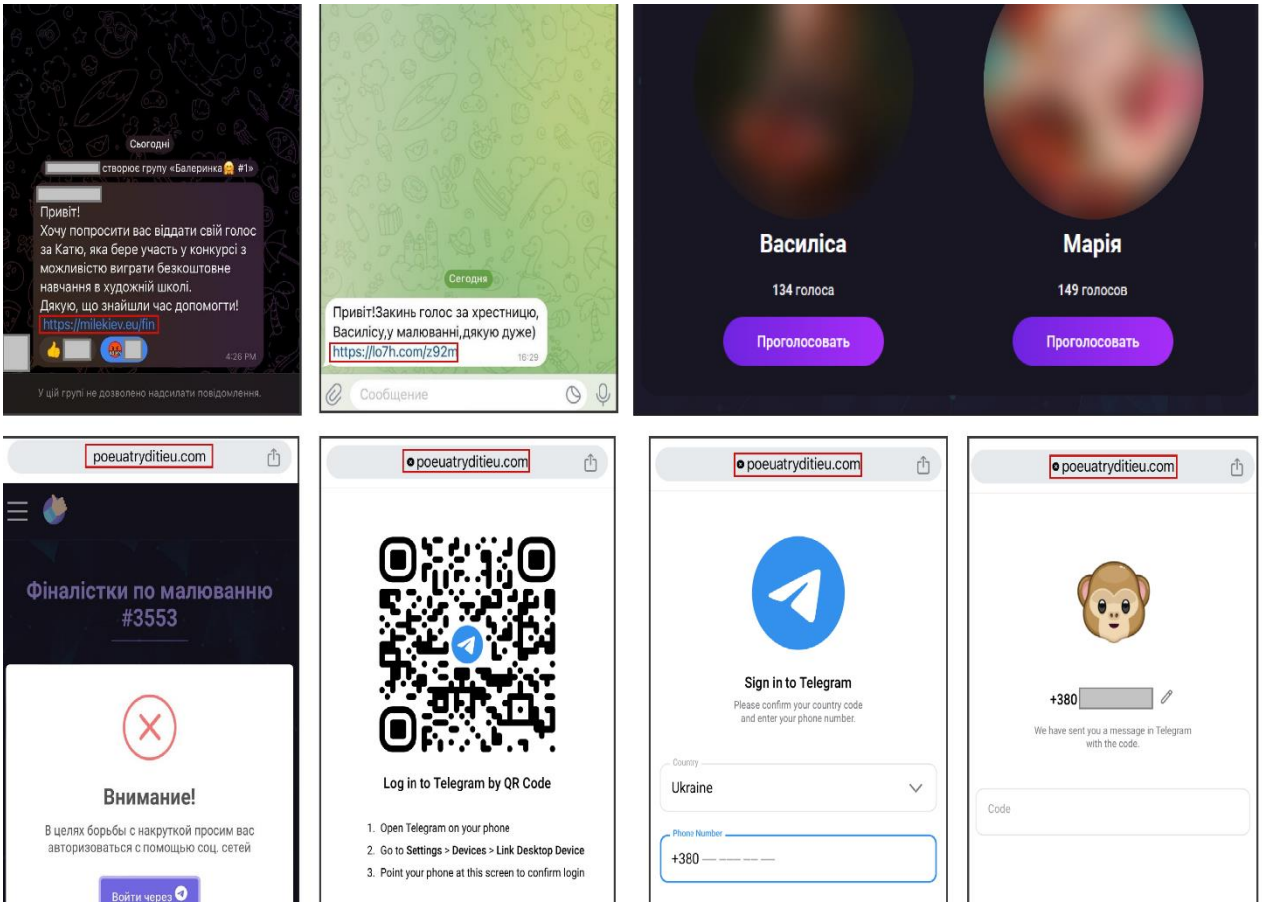
Шахраї зламують акаунти користувачів у Facebook, Instagram, Telegram, Viber та інші для подальшої розсилки повідомлень з проханням позичити грошей, поширення шкідливого програмного забезпечення та дезінформації.

Сценарії викрадення акаунтів у різних месенджерах та соціальних мережах:

- **Telegram**. Надходить повідомлення із посиланням на канал, який нібито повідомляє про години наявності електроенергії за обраною адресою. Якщо перейти за лінком, він перекидає на фішинговий акаунт ДТЕК або Yasno. Перед тим, як надати обіцяну інформацію щодо графіків вимкнення світла, бот запитує номер телефону. Одразу після цього надходить код для підтвердження входу на іншому пристрої. Бот просить його ввести. Якщо код буде введено і акаунт не захищено двофакторною автентифікацією, шахрай відразу отримує доступ до акаунту.



- **Telegram**. Розповсюджуються повідомлення з тематикою голосувань, що містять посилання на, нібито, конкурсні матеріали мистецької діяльності (образотворче, сценічне тощо). Отримувачу такого повідомлення пропонується відвідати вебресурс зі згаданими матеріалами, "авторизуватися" та підтримати конкурсанта. У випадку сканування QR-коду і/або введення номеру телефону та одноразового коду, до облікового запису жертви буде додано сторонній пристрій, після чого акаунт слід вважати скомпрометованим.



- **Signal.** Надходить сповіщення від акаунту з назвою Signal Support & Notification про вхід до облікового запису з нового пристрою. Щоб підтвердити, що це не ви, просять надіслати код з SMS. З цим кодом шахрай входить до облікового запису з нового телефону, а користувач втрачає доступ зі свого.
- **Facebook**. Шахраї розсилають лист нібито від Facebook щодо підозрілих дій в обліковому записі, пропонуючи користувачу перевірити безпеку. Посилання у листі переадресовує на фішинговий сайт Facebook, на якому користувачу пропонується ввести свій пароль та код двофакторної автентифікації. Після введення даних від Facebook відбувається злам та захват акаунту.
- **Instagram**. Надходить фішинговий лист із пропозицією начебто від Instagram отримати блакитний бейдж, тобто верифікувати акаунт. Оскільки власники акаунтів часто мріють отримати бейдж, адже це дає кредит довіри для їхньої аудиторії та дозволяє відрізнити справжній акаунт від фейкового. Після введення даних від Instagram відбувається злам та захват акаунту.

Поради, що працюють:

- Двофакторна автентифікація (2ФА) не захистить вашакаунт на 100%, – втім, від більшості поширених скамів вона допоможе.
  2ФА передбачає, що під час входу до облікового запису з нового пристрою та браузера месенджер / соціальна мережа, окрім пароля, вимагатиме додаткове підтвердження вашої ідентичності. Таким підтвердженням може бути SMS з одноразовим кодом, застосунок для смартфона (iOS або Android), який автоматично генеруватиме такі коди, набір із 10 одноразових резервних кодів, які ви можете роздрукувати чи переписати в блокнот, фізичний ключ безпеки, який треба вставляти в USB-порт.
  Якщо зловмисник знає вашпароль, не маючи другого фактора (якогось із перерахованих вище), він не зможе зайти до вашого облікового запису.
  І навпаки: маючи лише другий фактор, зловмисник не отримає доступу до вашого облікового запису — йому також потрібно буде дізнатись вашпароль.

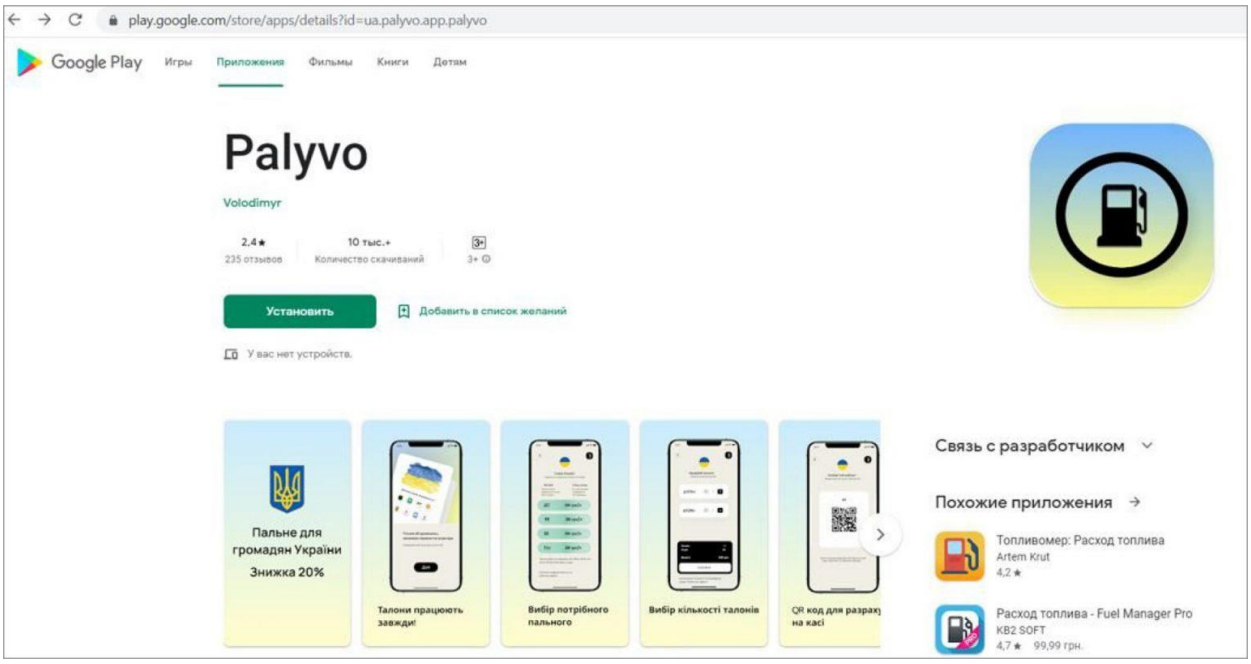
- Створюйте складні та унікальні паролі. Складні – це з літерами, цифрами та спеціальними символами. Пароль повинен бути унікальним та не містити персональної інформації про вас.
- Перевіряйте у налаштуваннях активні сесії (пристрої) та видаляйте ті, якими не користуєтесь.
- Перевіряйте електронну пошту та SMS. Коли ви реєструєтеся у соціальній мережі або месенджері, то прив'язуєте до облікового запису свій e-mail та телефон, на які сервіси надсилають автоматичне повідомлення про вхід до облікового запису з нового пристрою.
- Виходьте з облікового запису, якщо він вам не потрібен. Наприклад, якщо ви плануєте продавати свій смартфон або ноутбук, потрібно обов'язково вийти зі всіх облікових записів і видалити збережені паролі.
- Перед тим, як ввести облікові записи до соціальної мережі, перейшовши за отриманим посиланням, перевірте його через функціонал CheckMyLink або VirusTotal, який за лічені секунди безкоштовно перевірить посилання на шахрайство та віруси.
- Налашуйте надійні способи блокування екрану пристрою (PIN, пароль, TouchID, FaceID) та увімкніть приховування вмісту сповіщень на заблокованому екрані (Налашування телефону – Сповіщення).

5. Мобільні застосунки

Шахраї створюють та розміщують у Google Play та App Store фейкові мобільні застосунки, в які жертва сама вводить реквізити платіжної картки, або застосунки, що завантажують мобільні трояни, які отримують доступ до онлайн-банкінгу або криптогаманця.

Фіктивні мобільні застосунки, виявлені у Google Play та App Store минулого року:

- Фейковий застосунок Palyvo, що рекламується як застосунок для реалізації залишків палива за низькими цінами. Начебто за допомогою нього можна придбати універсальний спецталон у мережі OKKO, WOG, AMIC, BRSM, KLO, AVIAC, що «відварюється завжди» (лексика збережена). Також реклама застосунку обіцяє використання швидкого та зручного інтерфейсу, – з цим, дійсно, не обманюють, оплата здійснюється миттєво, але, далебі, – ні грошей, ні «універсального» талону.



- Фейковий застосунок Компенсації для громадян 2022 пропонує отримати компенсацію на платіжну картку із заблокованих ресурсів росії, виманюючи гроші начебто за сплату банківської комісії за перерахування грошей та карткові реквізити.

Користувачі, які бажають встановити на свій смартфон мобільний застосунок банку, вводять у пошукову систему характерний запит формату «завантажити застосунок банку ХХХ». Першою в пошуковій видачі з'являється платна реклама фіктивного банківського застосунку, в якому захований банківський троян. Після отримання відповідних дозволів, у тому числі на читання та відправлення SMS-повідомлень, встановлений фейковий застосунок запитує логін та пароль від особистого кабінету та реквізити платіжної картки. Таким чином, жертва, яка ні про що не підозрює, дає зловмисникам доступ до своїх конфіденційних даних, які використовуються для проведення банківських операцій в особистому кабінеті, зокрема грошових переказів. Водночас жертва ні про що не здогадується, оскільки SMS-повідомлення про доступ до її рахунку та операції перехоплюються банківським трояном.

Поради, що працюють:

- Посилання для завантаження банківського застосунку вказане на офіційному сайті банку – використовуйте лише його.
- Завантажуйте мобільні застосунки лише з офіційних сторів Google Play та App Store, але будьте пильними, – в офіційних сторах також зустрічаються фіктивні застосунки.
- Обов'язково перевіряйте, хто автор застосунку та чи має він відношення до реального бренду.
- Уважно вивчайте відгуки, – нерідко саме там можна зустріти попередження щодо шахрайства. Аналізуйте кількість завантажень застосунку.
- Варто пам'ятати, що обіцянка вигоди (знижки, грошова винагорода, вигідніші умови тощо) – характерна ознака шахрайства.
- Не давайте зайвих прав застосунку і завжди перевіряйте, які права він вимагає для своєї роботи.