Основные способы совершения киберпреступлений

СТАТИСТИЧЕСКИЕ ДАННЫЕ О КИБЕРПРЕСТУПНОСТИ

за 2023 - 2,6 млн. рублей
за 2024 – более 1,4 млн. рублей

Еженедельно около 380 преступлений

Третья часть регистрируется в Минске

Самым возрастным потерпевшим по 86 лет, они установили приложение

Портрет ЖЕРТВЫ киберпреступника

женщины (60%)
от 31 до 45 лет (33,2%)
трудоустроены
с высшим образованием (40%)

Способы совершения

Мошенничества 60%

Хищения имущества, путем модификации комп. инф. 30%

Незаконный оборот средств платежа 4,1%

Несанкционированный доступ, уничтожение, блокирование, модификация и иные 3,9%

Вымогательства 3,3%

Заведомо ложное сообщение об опасности 1,6%

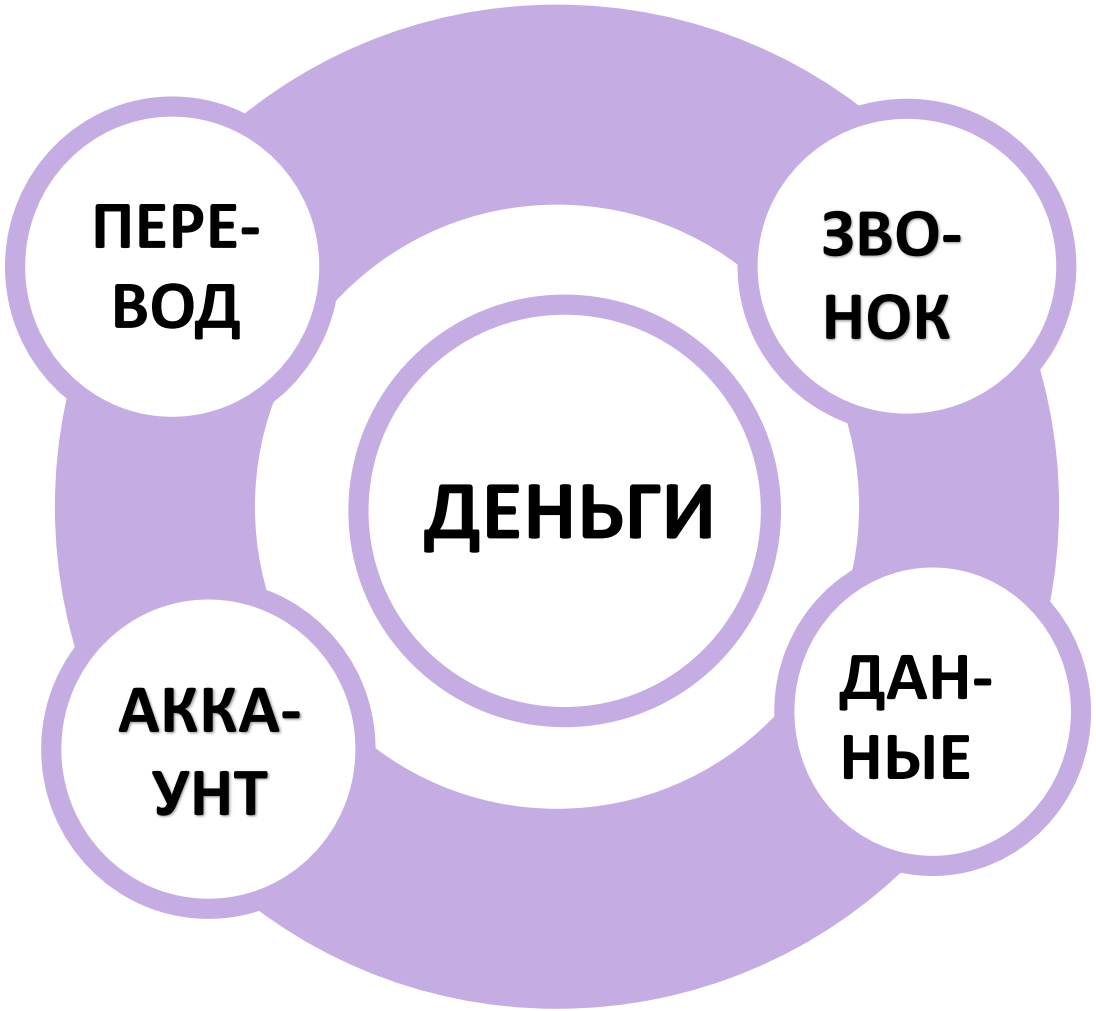
Интернет-мошенничества и хищения с использованием сети Интернет составляют более 90% от всех киберпреступлений

Реклама в мессенджерах, сообщение в соцсетях

Владельцы **сами** переводят деньги за несуществующий товар, доверяя рекламе в Интернете, или после сообщения (текстового или голосового) с просьбой родственника или знакомого из социальной сети..

Доступ к аккаунту

После завладения одним аккаунтом мошенники с него рассылают другим контактам **фейковые** голосовые или текстовые сообщения с просьбой перевести деньги.



Звонок в мессенджере

Мошенники представляются сотрудниками правоохранительных органов, банковских организаций, работникаами операторов связи, родственниками.
Убеждают установить программное обеспечение, получить кредит, перевести деньги на «защищенный счет».

Получение персональных данных

ФИШИНГ поддельные сайты банков, криптобирж или мобильные приложения операторов связи.
Получив личные данные или деньги, похищают их.

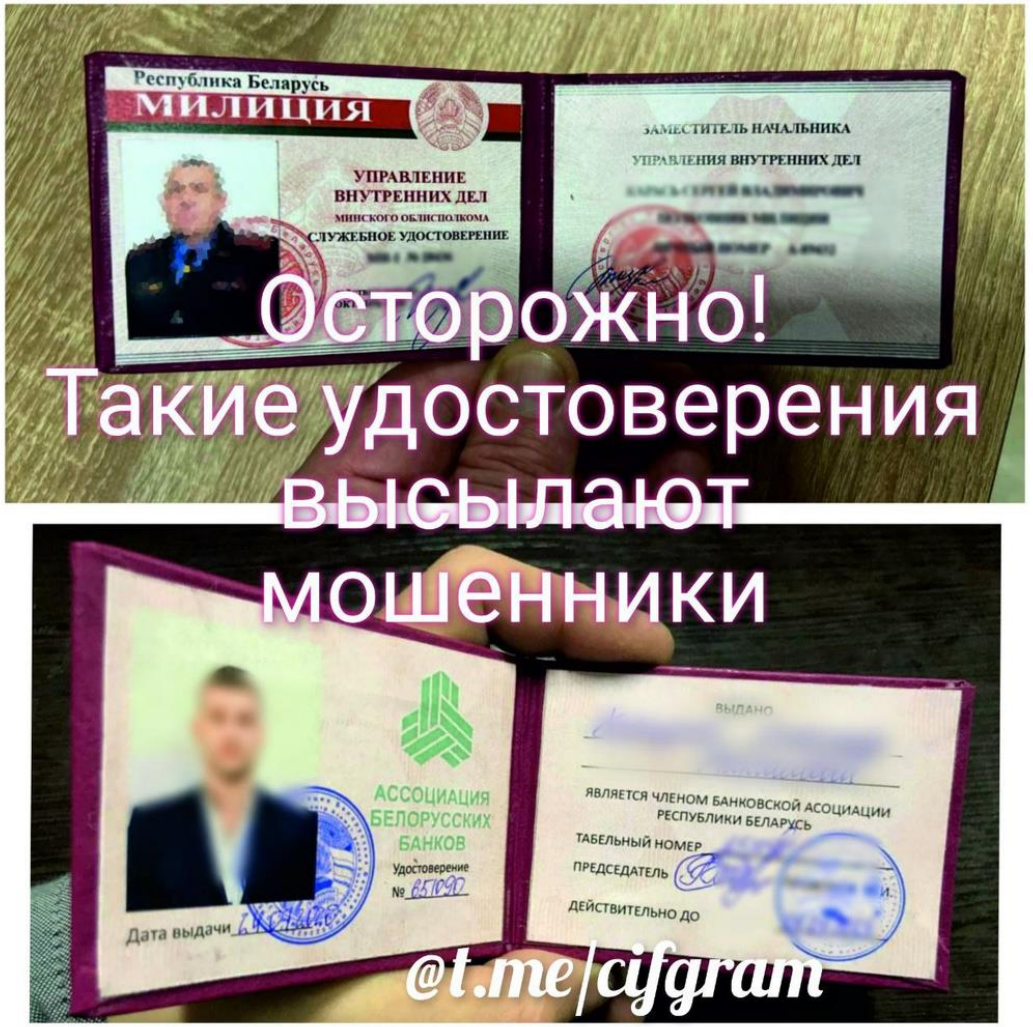
ВИШИНГ

Суть схемы

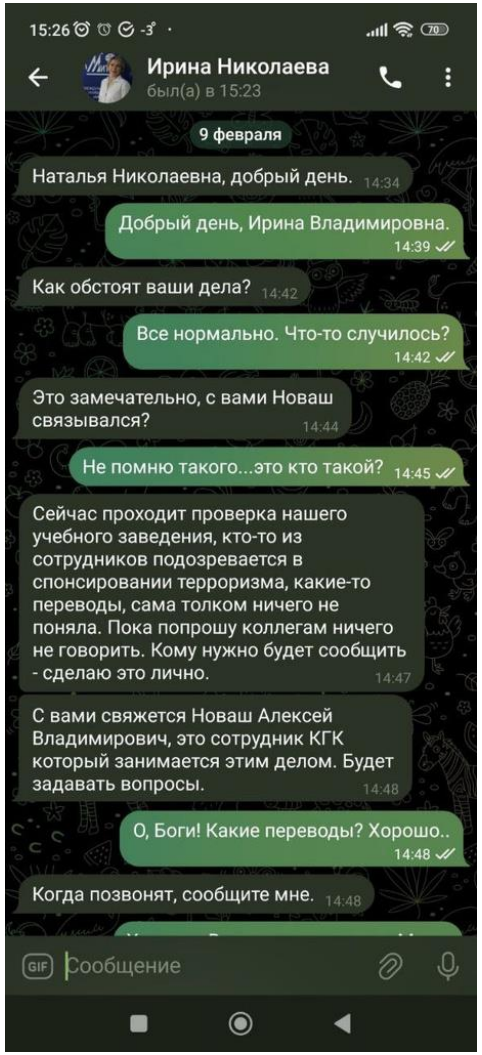
Мошенники представляются сотрудниками правоохранительных органов, работниками банка, операторов связи или госорганов.

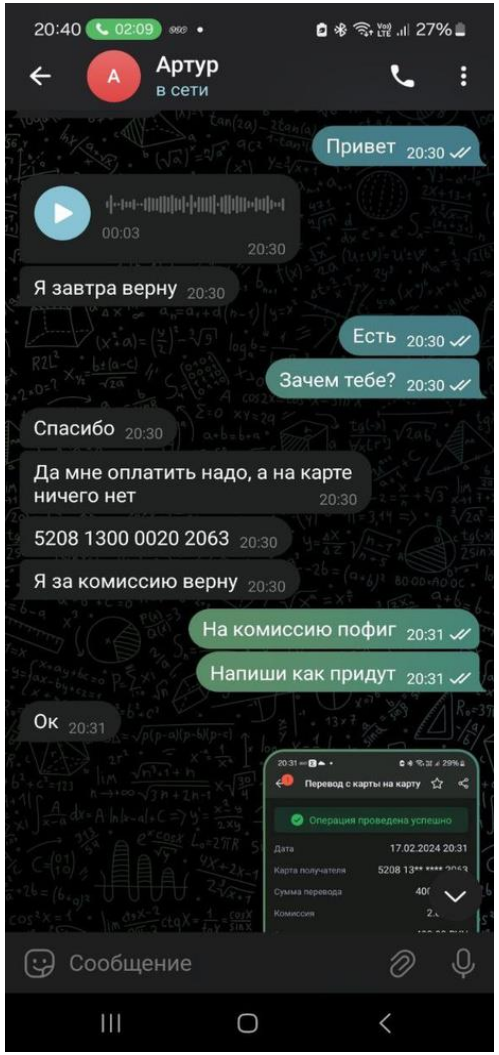
Используют психологические уловки, играют на чувствах, сначала угрожают или сообщают о проблеме, потом предлагают помощь в ее решении.

Убеждают установить программное обеспечение и передать код регистрации, или получить кредит и перевести деньги на “защищенный” счет.



Создают новый аккаунт и текстовые (голосовые) сообщения от имени знакомых для побуждения к выполнению действий другого мошенника, который может представиться сотрудником госорганов (1-2). Или голосом друга попросить денег (3).





Чтобы НЕ СТАТЬ ЖЕРТВОЙ
киберпреступника,
как можно раньше
ЗАКОНЧИТЕ РАЗГОВОР
с неизвестным лицом
кем бы он не представился.

Создают фейковые сайты криптобирж или инвестиционных платформ.

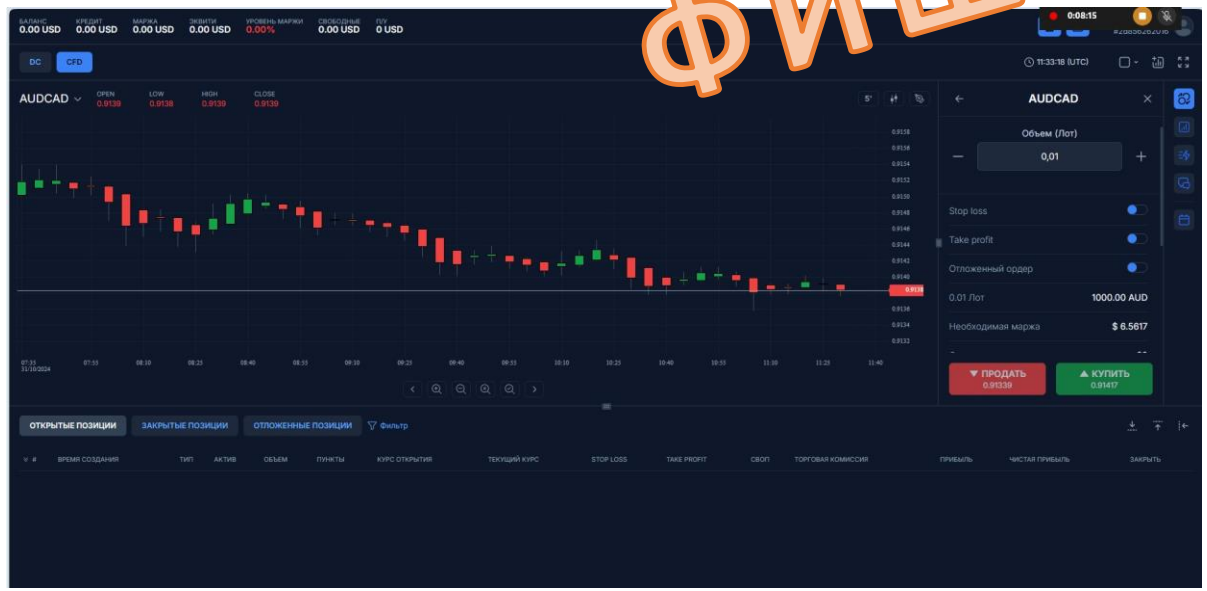
Суть схемы

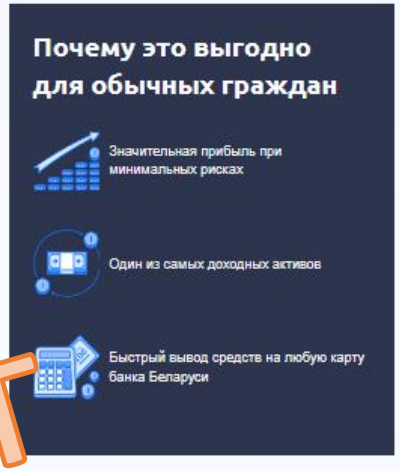
Мошенники создают поддельные сайты криптобирж или инвестиционных платформ. Размещают рекламу в Интернете. Подыскивают заинтересованных в пассивном доходе людей, готовых вложить реальные деньги в фейковую биржу, якобы под «руководством куратора».
На деле оказывается, что заработок, видимый на экране, всего лишь нарисованный.

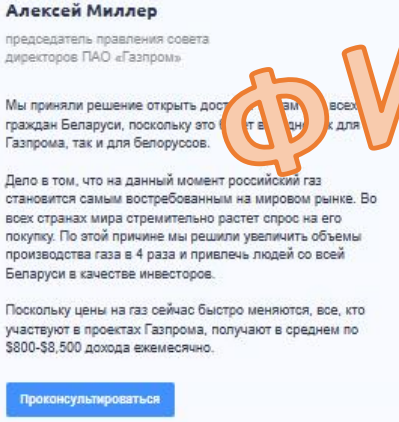
1. Отклик на рекламу и заполнение формы обратной связи.
2. Звонок от куратора (трейдера) с предложением вложить деньги в инвестиции. Иногда может быть по мобильной связи.
3. При попытке вывода денег с биржи необходимо оплатить взносы, налоги, комиссию, пошлину и прочие платежи.

Легких денег НЕ БЫВАЕТ.
Реклама инвестиций работает по принципу финансовой пирамиды.

ПРИМЕРЫ ПОДДЕЛЬНЫХ ПЛАТФОРМ







Создают фейковый магазин или аккаунт на торговой площадке

Суть схемы

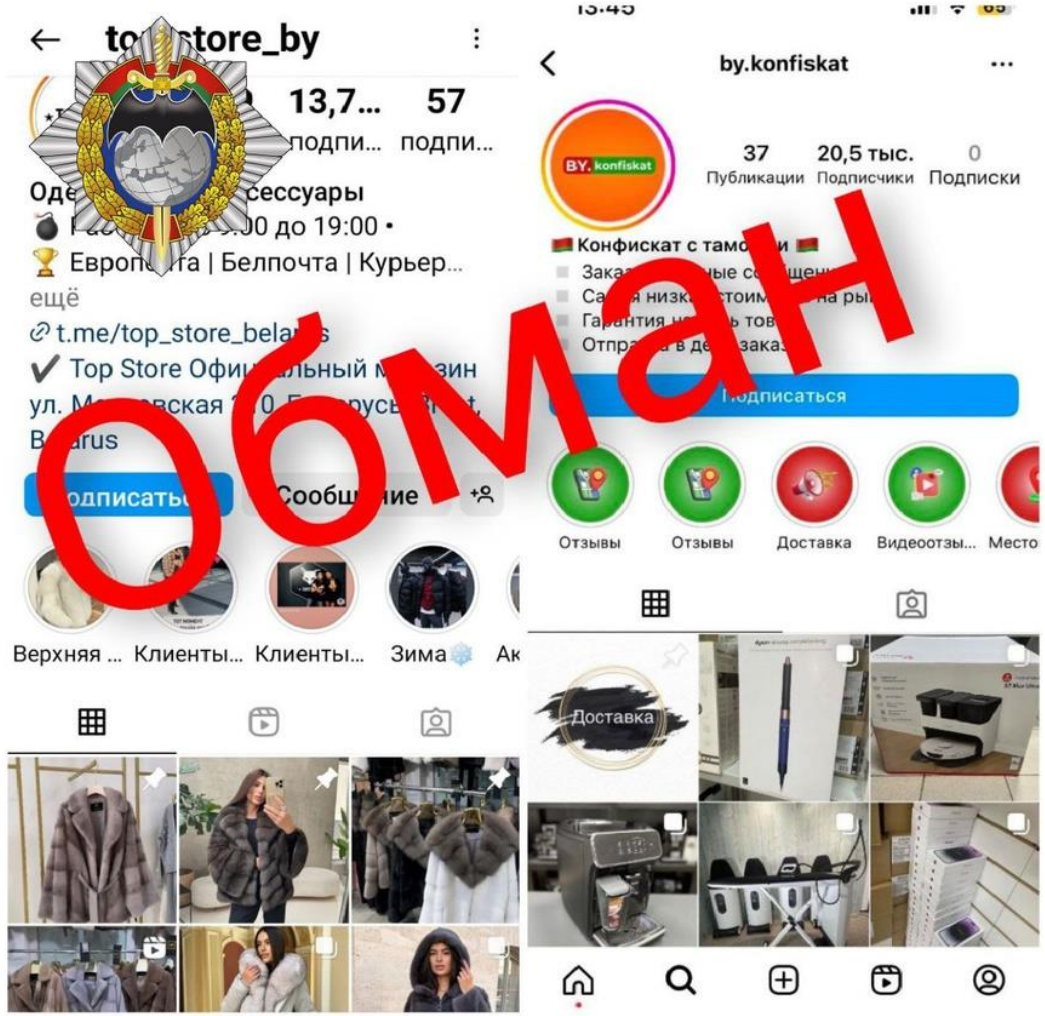
Мошенники создают аккаунты в соцсетях и на торговых площадках.

Размещают фото товара по заниженной стоимости.

И под различными предлогами убеждают перевести денежные средства в качестве полной или частичной предоплаты.

Проверьте существование магазина, **позвонив по белорусскому номеру,**

оцените дату создания аккаунта и насторожитесь большим количеством подписчиков за короткое время.



Создают фейковые сайты банков

Фишинг.
Способ, когда мошенники точно копируют настоящий и создают фишинговый сайт.
Чаще всего завладевают персональными данными, используя поддельные страницы **банков, театров, кальянных.**

При входе в зеркальный интернет-банкинг или при покупке «билетов» на фишинговом сайте пользователь вводит свои личные данные, в том числе код из СМС.

Этими данными **завладевают мошенники** и **совершают хищение** денежных средств.

Интернет-адреса белорусских организаций располагаются в национальном сегменте Интернета – доменной зоне «**BY**».

ВСЕГДА ПРОВЕРЯЙТЕ АДРЕС СТРАНИЦЫ, ГДЕ ВВОДИТЕ ЛИЧНЫЕ ДАННЫЕ.

Интернет-адрес официальной страницы https://ibank.asb.by/

ПОЛЬЗУЙСЯ БЕЗОПАСНО

https:// оплата .by/
https:// банк
https:// доставка

- Пользуйтесь мобильными приложениями банка
- Переходите в интернет-банкинг только с официального сайта банка
- Проверяйте адрес интернет-банкинга в адресной строке, между последней точкой и первой наклонной чертой должно быть только так .by/
- Активируйте на карте, используемой для онлайн-платежей, услугу 3-D Secure (подтверждение платежей SMS-кодом)
- Не переходите в интернет-банкинг по ссылкам в поисковых системах
- Не используйте SMS-коды от банка и код с оборотной стороны карты для получения денежных средств
- Не переходите по ссылкам из сообщений для доступа к интернет-банкингу и иным сервисам или услугам

УПРАВЛЕНИЕ
ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ
УВД ВИТЕБСКОГО
ОБЛИСПОЛКОМА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Денежные переводы

Мошенники под различными предлогами “вытягивают” из жертв деньги.
Фейковые магазины предлагают перевести предоплату за товар на счет или БПК.

Коды из сообщений

Цифровые коды из СМС в совокупности с другими данными предоставляют **доступ к сервисам** и, в некоторых случаях, дают возможность оформить онлайн-кредит.

Личные данные

Ограничьте распространение личных данных Мошенники используют нейросети и создают дип-фейки (голосовые или видеоизображения).

Облачные пароли

К разным сервисам разные пароли
Состав пароля
Менеджер паролей
Облачные пароли (двухфакторная аутентификация) к сервисам.

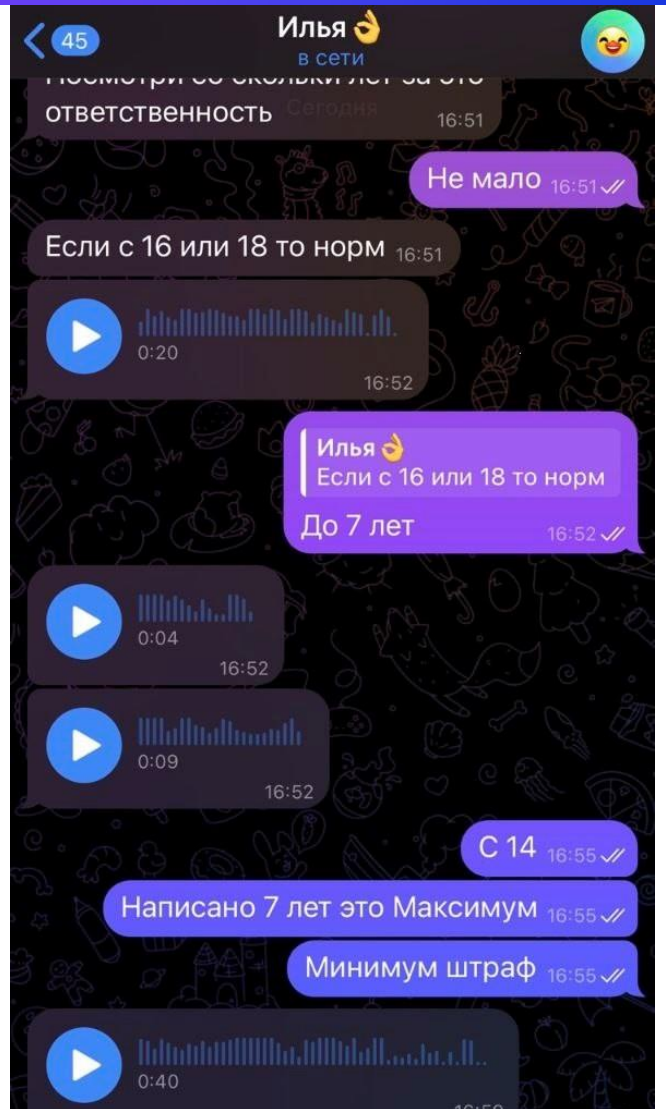
СВАТИНГ. Ложное сообщение об опасности.

Тренд распространяется в молодежной киберсреде.

Суть схемы

Заключается в том, чтобы создать неблагоприятную обстановку госорганам, нарушить режим их работы или отомстить своему обидчику, создав для него проблемы с правоохранительными органами.

Ответственность наступает с 14 лет и предусматривает вплоть до 7 лет лишения свободы.



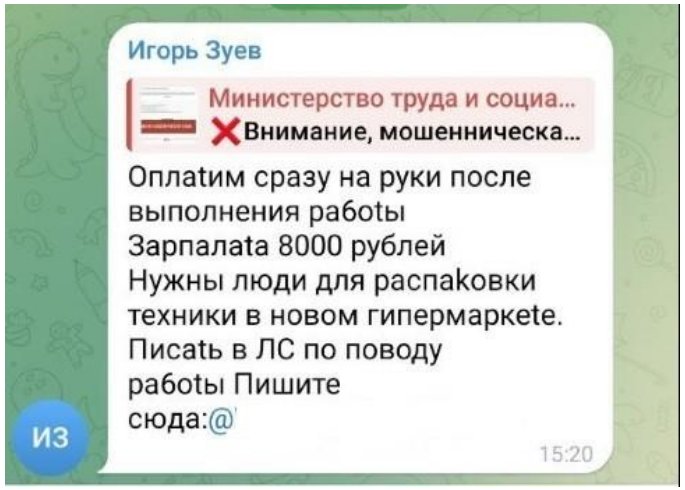
ВОВЛЕЧЕНИЕ В Киберпреступность

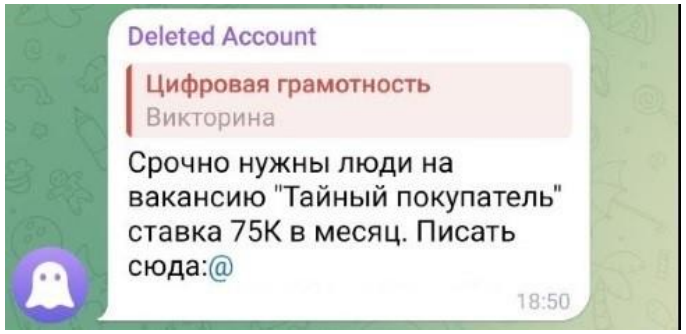
Дропы – люди, предоставляющие свои банковские реквизиты для того, чтобы через их промежуточные счета проводились похищенные деньги.

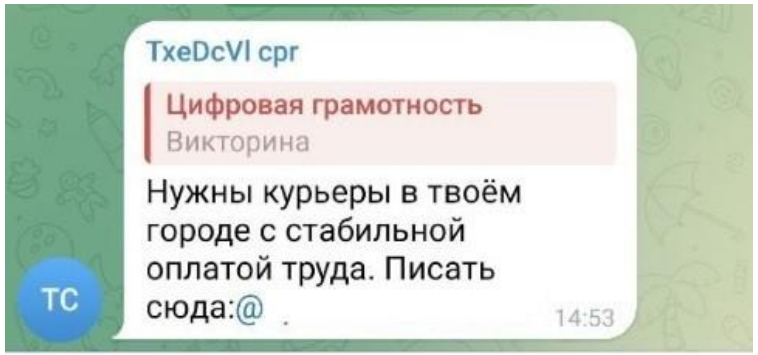
Для поиска дропов мошенники размещают различные объявления с вакансиями.

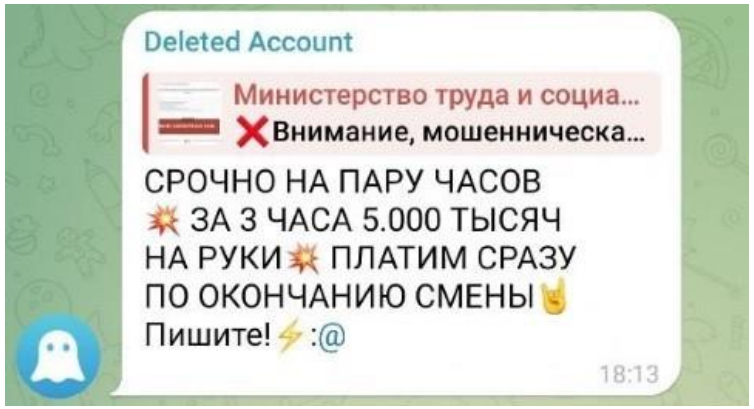
Ответственность за происхождение прошедших по банковским счетам денег несут владельцы таких счетов.

Статьей 222 УК предусмотрено наказание вплоть до 10 лет лишения свободы.









ОПЕРАЦИИ С КРИПТОВАЛЮТОЙ

РАЗРЕШЕНО

Покупать токены (криптовалюту) за денежные средства только на белорусских криптобиржах, являющихся резидентами Парка высоких технологий.

Обменивать токены на другие токены на любых криптоплатформах без ограничений.

ЗАПРЕЩЕНО

Покупать или продавать токены (криптовалюту) за денежные средства на иностранных криптобиржах и у физических лиц.

Порядок осуществления
сделок с криптовалютой определен
Указом Президента от 17.09.2024 №367
«Об обращении цифровых знаков (токенов)»

Будьте бдительны!
Эти знания помогут вам сохранить ваши деньги!

Главное управление
по противодействию киберпреступности
криминальной милиции
МВД Республики Беларусь.