Управление по противодействию киберпреступности
криминальной милиции
УВД Витебского облисполкома

СОВРЕМЕННАЯ КИБЕРПРЕСТУПНОСТЬ

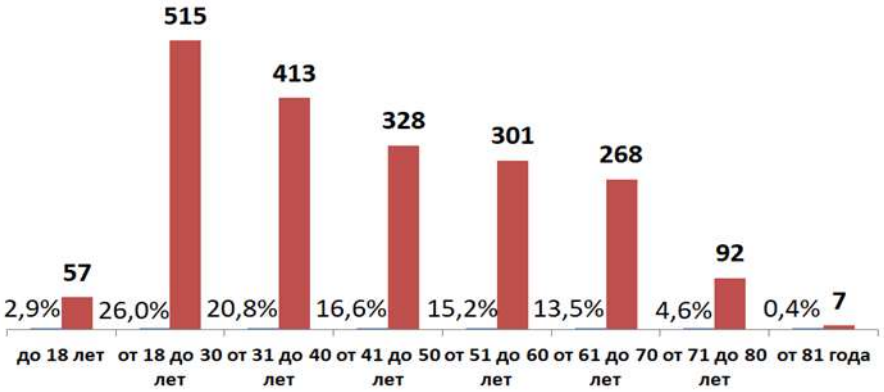


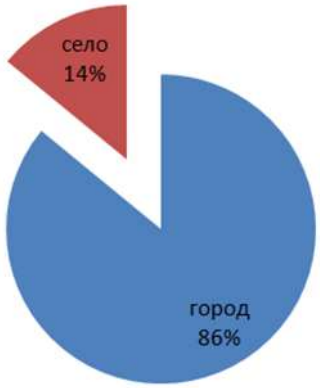
г. Витебск, 10 марта 2025 г.

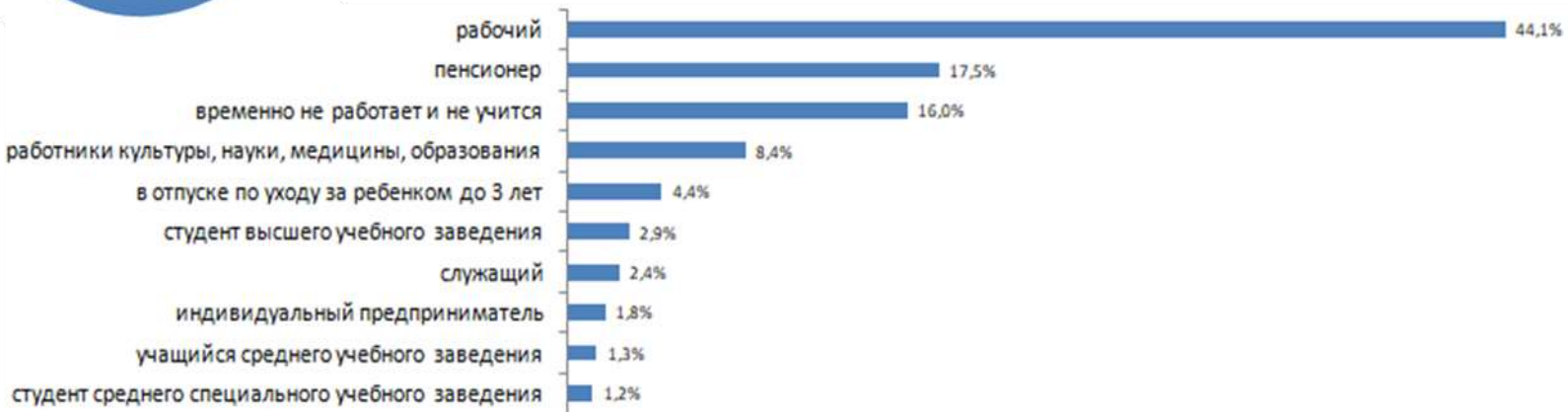
Основные категории потерпевших

(сведения за 2024 год)









Количество киберпреступлений в стране



В 2024 г. киберпреступления составили 27,5% от всех зарегистрированных.

Третья часть совершается в г. Минске.

Ежедневно в 2025 - около 40 киберпреступлений, в 2024 – 55, в 2023 – 50.

Мошенничества и хищения имущества составляют более 80% от всех киберпреступлений

Доступ к аккаунту

Владельцы сами предоставляют доступ к своим аккаунтам, после чего с их учетной записи **рассылаются сообщения** с просьбой денег в долг или оказать помощь больному человеку.

Звонок в мессенджере

Мошенники представляются сотрудниками правоохранительных органов, банковских организаций, родственниками, руководителями. **Могут убедить** установить программное обеспечение, получить кредит, перевести деньги на «защищенный счет».



Telegram-канал "Цифровая грамотность"

@cifgram

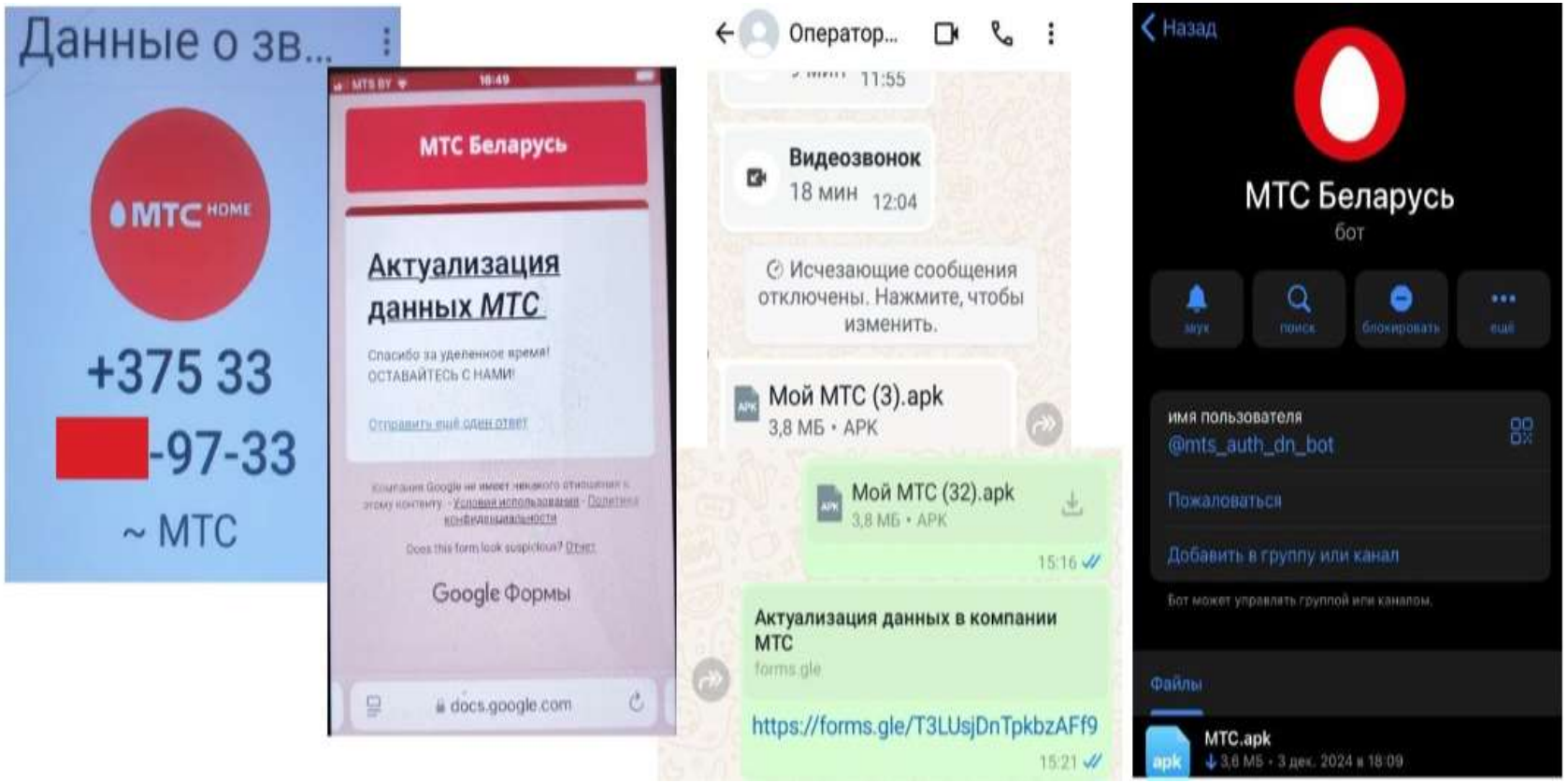
Сообщение в соцсетях или мессенджере

Создают фейковые **магазины, криптобиржи,** . Используя **искусственный интеллект** мошенники создают изображения или голосовые сообщения с просьбой перевести деньги.

Получение персональных данных

ФИШИНГ поддельные сайты банковских организаций или криптобирж.
Получив личные данные, похищают деньги или открывают счета и проводят похищенные деньги

Мошенники от имени операторов



Так выглядит сотрудник, который вам звонит (ВИШИНГ)

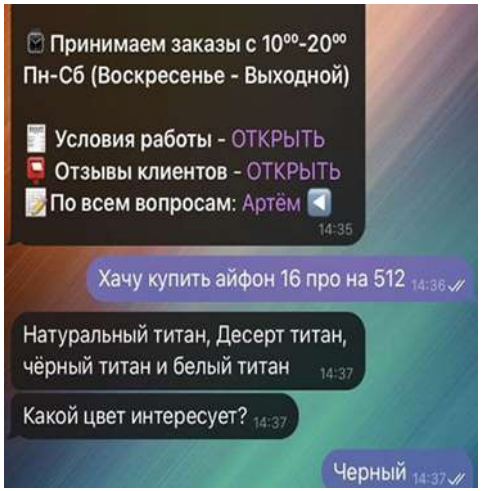
Мошенники используют психологические уловки, играют на чувствах, сначала угрожают или сообщают о проблеме, потом предлагают помощь в ее решении.

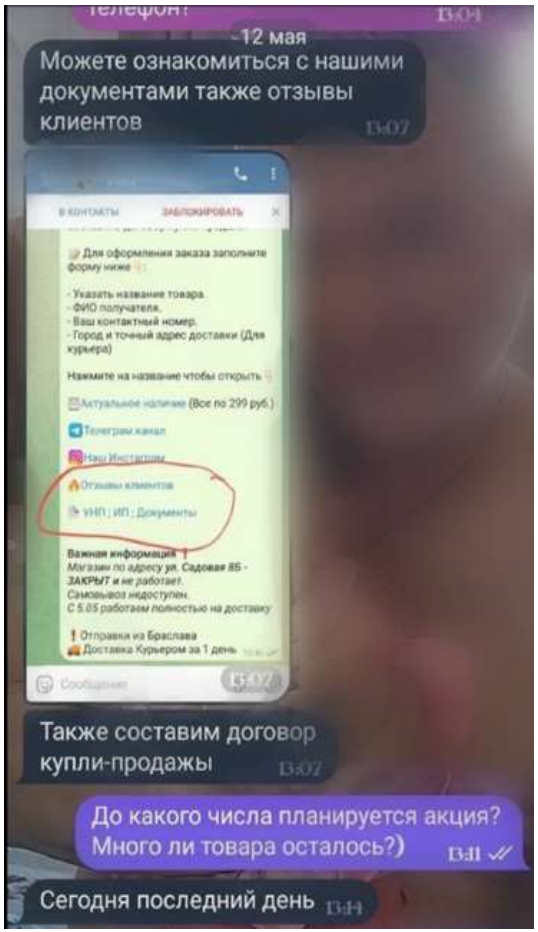
Потом убеждают установить программное обеспечение и передать код регистрации, или получить кредит и перевести деньги на “защищенный” счет



Мошенники создают фейковые магазины или аккаунты на торговых площадках

Мошенники создают странички в соцсетях и на торговых площадках.
Размещают фото товара по заниженной стоимости.
И под различными предлогами убеждают перевести денежные средства.
Рекомендуется проверить существование магазина, позвонив по белорусскому номеру.





Мошенники создают фейковые сайты криптобирж или инвестиционных платформ

Мошенники создают сайты криптобирж или инвестиционных платформ. 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.

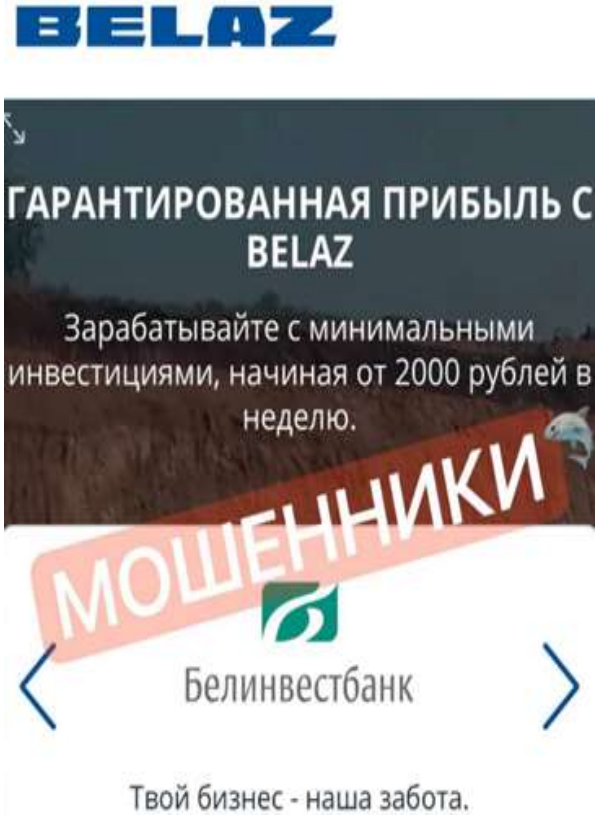
Легких денег НЕ БЫВАЕТ.
Реклама инвестиций работает по принципу финансовой пирамиды





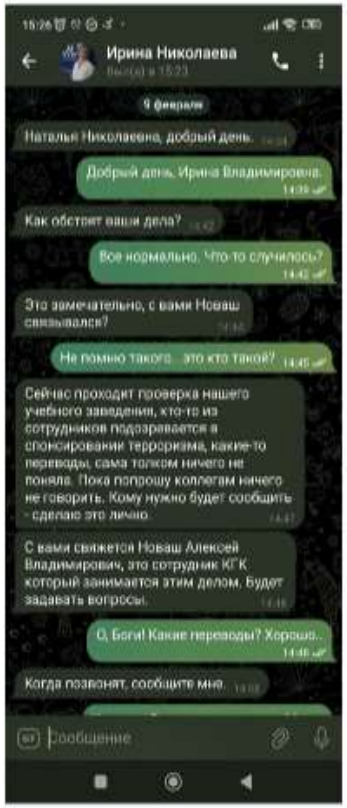
Не упустите возможность стать участников проекта от БелТрансГаз, ведь для этого нужно выполнить один простой шаг и 2 минуты Вашего времени.

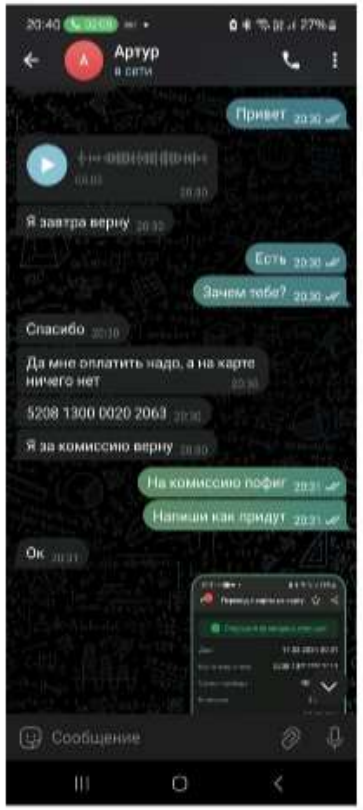

GREAT STONE
Менеджер Виктория
Великий камень
Здравствуйте, я - ваш персональный менеджер Алиса! **Поздравляю!**🏆 «Великий камень» открывает перед вами возможность зарабатывать на народных ресурсах и получать доход в размере **от 5000 рублей** уже с первых недель! Вам нужно ответить на пару вопросов, и внести минимальный депозит, чтобы я смогла оказать вам помощь и приступить к работе!
18:59


BELAZ
ГАРАНТИРОВАННАЯ ПРИБЫЛЬ С BELAZ
Зарабатывайте с минимальными инвестициями, начиная от 2000 рублей в неделю.
МОШЕННИКИ
Белинвестбанк
Твой бизнес - наша забота.

Мошенники создают новый аккаунт и текстовые (голосовые) сообщения от имени знакомых для побуждения к выполнению действий другого мошенника, который может представиться сотрудником госорганов.







Telegram-канал “Цифровая грамотность”
@cifgram

Фейковый конкурс рисунков по ссылке “друга”







СУТЬ схемы

Создается фишинговый сайт, ссылку на который рассылают контактам владельца аккаунта. В некоторых случаях рисунки **создаются нейросетью**.

Пользователю предлагается кликнуть кнопку голосования, ввести свой номер телефона и код, поступивший в уведомлении.

После ввода таких данных мошенники получают доступ к очередному аккаунту, с которого продолжают реализовывать другие мошеннические схемы, в том числе для рассылки сообщений о помощи больным детям.

Фишинг.

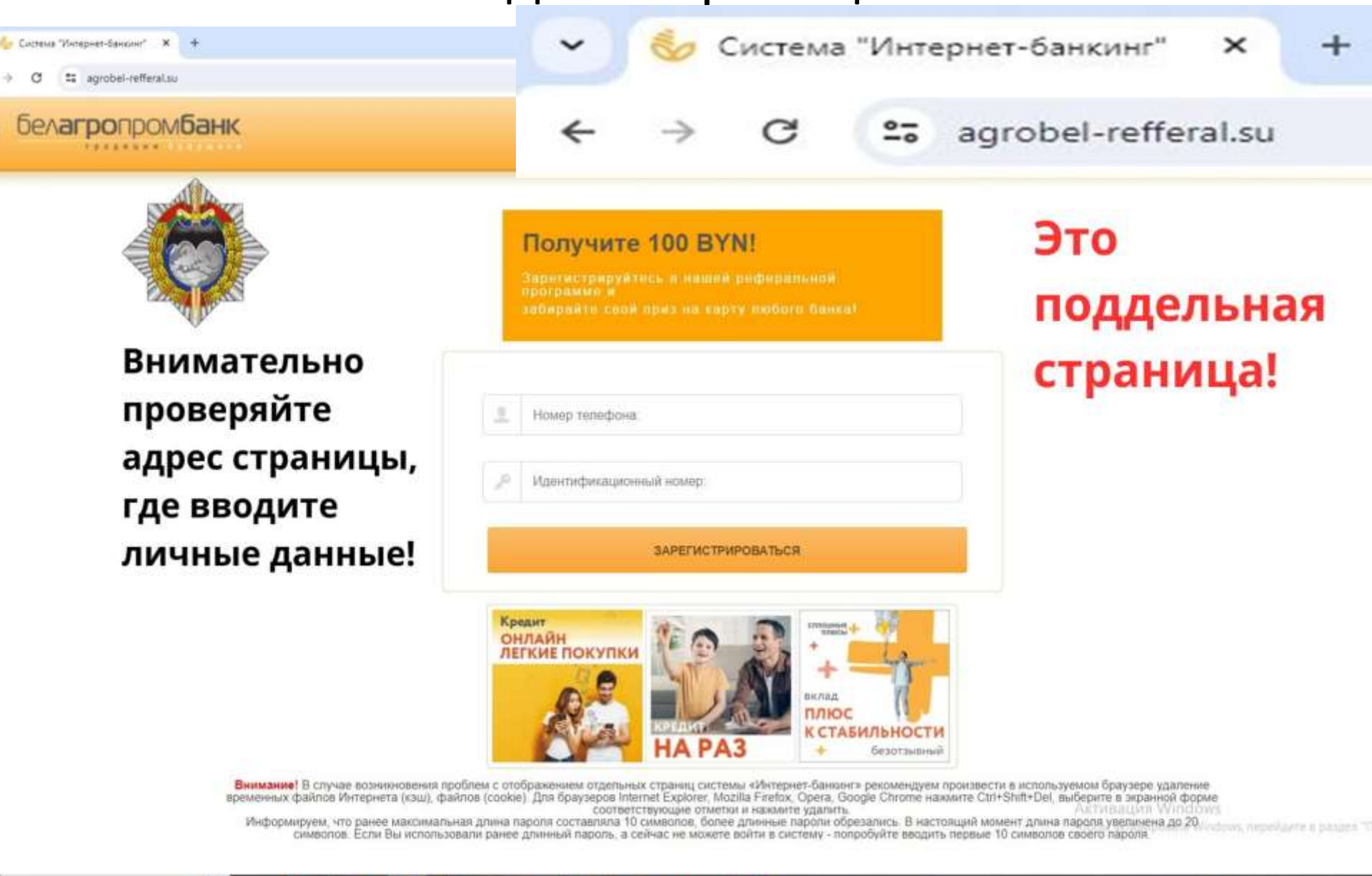
Способ, когда мошенники завладевают персональными данными и совершают хищение денежных средств.

Мошенник точно копирует настоящий и создает фишинговый сайт.

Интернет-адреса белорусских организаций должны быть расположены в национальном сегменте Интернета – доменной зоне «.BY» или «.бел».

Всегда проверяйте адрес страницы, где вводите личные данные.

Мошенники создают страницы-клоны банков



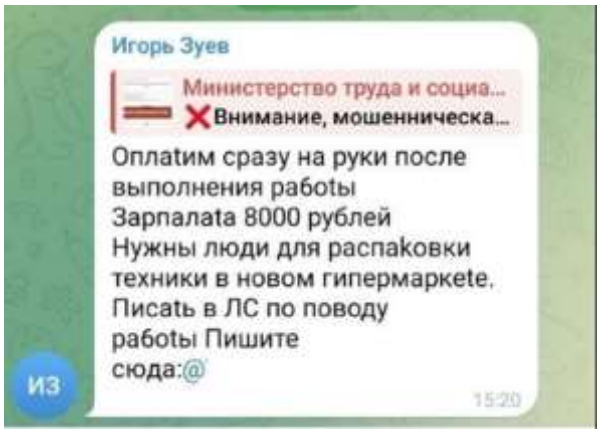
Внимательно проверяйте адрес страницы, где вводите личные данные!

Это поддельная страница!

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.

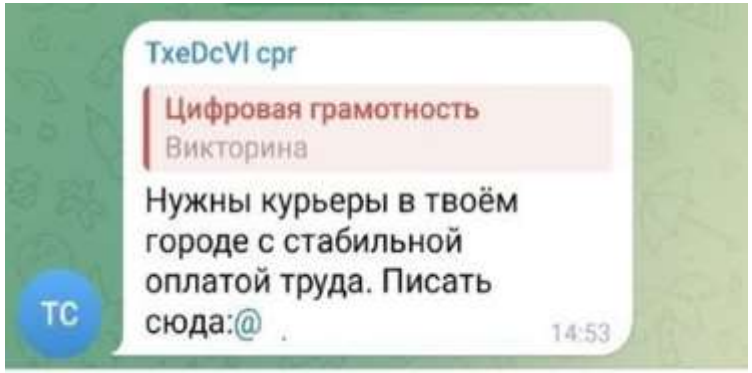


Ответственность за происхождение прошедших по банковским счетам денег несут владельцы таких счетов.



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





Информационная безопасность



Сложные пароли

К разным сервисам разные пароли
Состав пароля
Менеджер паролей
Облачные пароли к сервисам



Коды и ключи

Коды в совокупности с другими данными предоставляют доступ к сервисам и, в некоторых случаях, дают возможность оформить кредит.



Денежные переводы

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



Личные данные

Распространение личных данных способствует совершению преступлений.
Мошенники используют нейросети и создают дип-фейки (голосовые или видеоизображения).

Наши рекомендации





Телеграмм-канал “Цифровая грамотность”

Канал о том, как не стать жертвой мошенников в интернете и почему важна цифровая гигиена.

Для подписки на канал наведите камеру мобильного телефона на QR-код