Основные виды интернет мошеннечества

ЗВОНКИ ОТ ИМЕНИ БАНКОВ ИЛИ ГОС.СЛУЖАЩИХ:

Мошенники все чаще прибегают к использованию искусственного интеллекта для искажения голосов и лиц с целью обмана. Часто они представляются государственными сотрудниками или сотрудниками банка, предупреждая о подозрительных операциях.
Важно помнить, что правоохранительные органы никогда не будут требовать выполнения каких-либо действий по телефону.

ФИШИНГОВЫЕ САЙТЫ:

Мошенники создают поддельные сайты для сбора ваших данных. Будьте осторожны с переходом по незнакомым ссылкам, особенно связанным с покупками или доставкой.

МОШЕННИЧЕСТВО ПРИ ПОКУПКАХ В **INSTAGRAM:**

В настоящее время онлайн-покупки в магазинах **Instagram** становятся все более популярными, за что активно принимаются мошенники, создавая фальшивые магазины, требуя предварительную оплату и исчезая. Важно тщательно проверять продавцов, не доверять слишком низким ценам и не осуществлять переводы на личные счета.

МОШЕННИЧЕСТВО НА ТОРГОВЫХ ПЛОЩАДКАХ:

Мошенники могут попытаться получить предоплату за товар, а затем исчезнуть. Рекомендуется тщательно проверить подлинность товара и отзывы о продавце перед совершением покупки.

ИНВЕСТИЦИОННЫЕ СХЕМЫ:

Преступники могут предложить вам инвестировать в криптовалюту или акции, обещая высокие доходы. Изначально они могут вернуть вам небольшие суммы, но затем попросить увеличить ваши инвестиции, после чего скрыться с вашими деньгами.

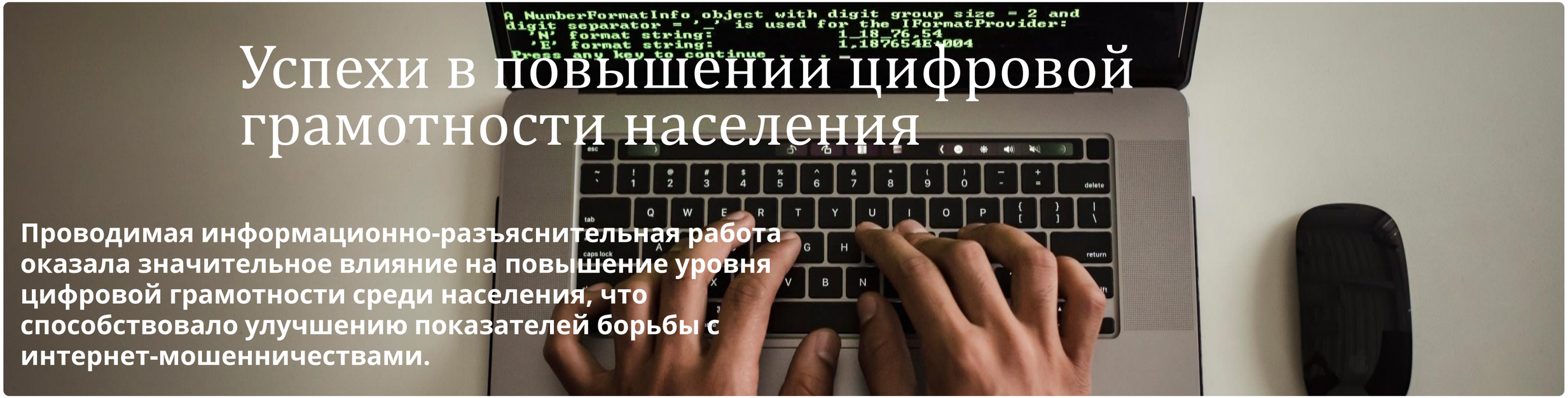
ВЗЛОМ АККАУНТА **WHATSAPP:**

Злоумышленники используют вредоносные ссылки для несанкционированного доступа к вашей учетной записи, впоследствии отправляя запросы на финансовую помощь от вашего имени. Пожалуйста, проверьте список "Привязанные устройства" и активируйте двухфакторную аутентификацию для обеспечения безопасности вашего аккаунта.

***при выявлении противоправных действий необходимо обратится в полицию на короткий номер 102!!!**

Ваша бдительность поможет сохранить ваши сбережения!

Успехи в повышении цифровой грамотности населения



Проводимая информационно-разъяснительная работа оказала значительное влияние на повышение уровня цифровой грамотности среди населения, что способствовало улучшению показателей борьбы с интернет-мошенничествами.

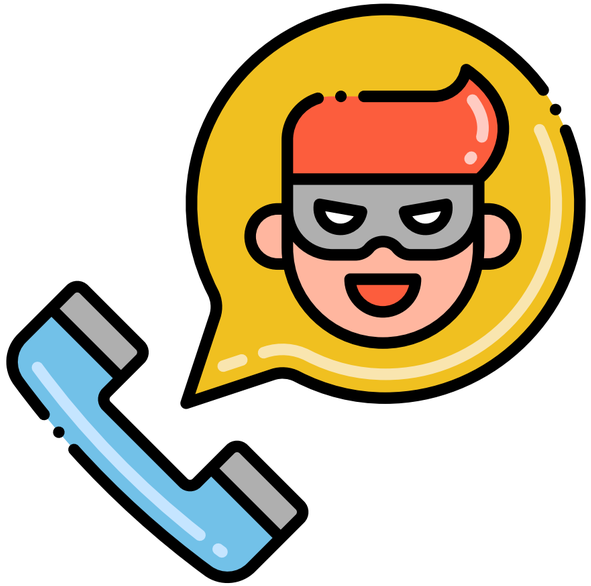
Снижение числа интернет-мошенничеств:
Благодаря активной информационной поддержке и обучению граждан удалось добиться сокращения числа случаев интернет-мошенничеств на **2,7%.** Конкретно, количество зарегистрированных инцидентов уменьшилось на **75** случаев, что соответствует снижению с **2 739** до **2 664** случаев.

Повышение раскрываемости преступлений:
Усиление осведомленности граждан и их способности распознавать мошеннические схемы способствовало росту эффективности работы правоохранительных органов. В результате, уровень раскрываемости интернет-мошенничеств увеличился на **2,8%**, что привело к росту показателя с **19,5%** до **22,3%.**

Эти результаты подчеркивают важность продолжения информационно-разъяснительной работы, направленной на обучение населения и предотвращение преступлений в цифровой среде.

Звонки от имени банков или гос.служащих:

звонки от имени сотрудников службы безопасности банков либо государственных служащих с использованием искусственного интеллекта – в котором составляется диалог по аудио либо видео связи, мошенниками монтируются не только голоса но и лица собеседников. Злоумышленники представляются сотрудниками полиции, национального банка либо знакомыми и близкими Вам людьми.
Могут вводить Вас в заблуждение под видом проведения сомнительных банковских транзакции либо проведения спецоперации по поимке злоумышленников.



Помните, полиция не привлекает граждан к задержанию злоумышленников по телефону, в том числе по видеосвязи.

Неправомерный доступ к аккаунту мессенджера **«What’s App»**

Злоумышленники используют вредоносную ссылку, которая как правила поступает от знакомых контактов. После прохождения по указанной ссылке они получают доступ к учетной записи, затем рассылают информацию всем контактам с просьбой одолжить денежные средства, которые выводятся на подставные банковские счета.

Продажа товаров и услуг в социальных сетях и торговых площадках:

Данный вид предусматривает мнимую реализацию различного рода товаров и услуг, где они всяческим образом будут подводить и просить перевести денежные средства в качестве предоплаты.

Лучше отказаться от таких сделок, до тех пор пока не увидите товар своими глазами, в противном случае Вы можете остаться без своих сбережений;

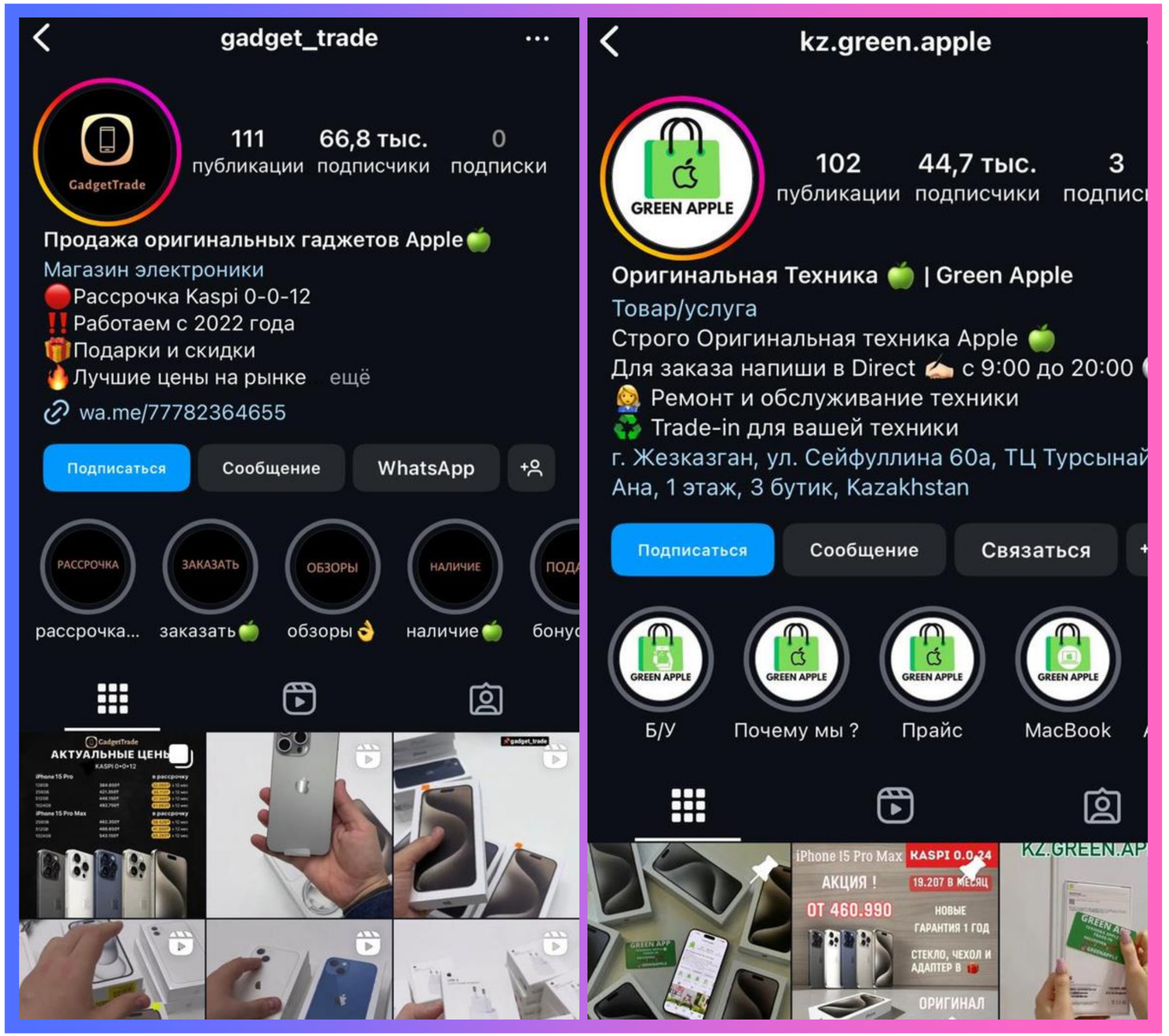
Мошенничество при покупках в **Instagram:**как не попасться

Хотелось бы отбратить внимание**!**

Продажа сотовых телефонов с фейковых аккаунтов**Instagram** является одним из более распространенных видов интернет-мошенничества**.** Злоумышленники создают поддельные профили, указывают слишком низкую цену для нового смартфона, зачастую выставляют электронные счета на оплату, имитируя себя за реальных продавцов, чтобы обмануть покупателей**.**

В связи с чем призываем граждан проявлять максимальную бдительность и выбирать оплату после получения товара, а также приобретать телефоны на проверенных торговых площадках**.**

Следуя этим рекомендациям, можно значительно снизить риск стать жертвой мошенников при покупке сотовых телефонов через **Instagram.**



Использование фишинговых сайтов

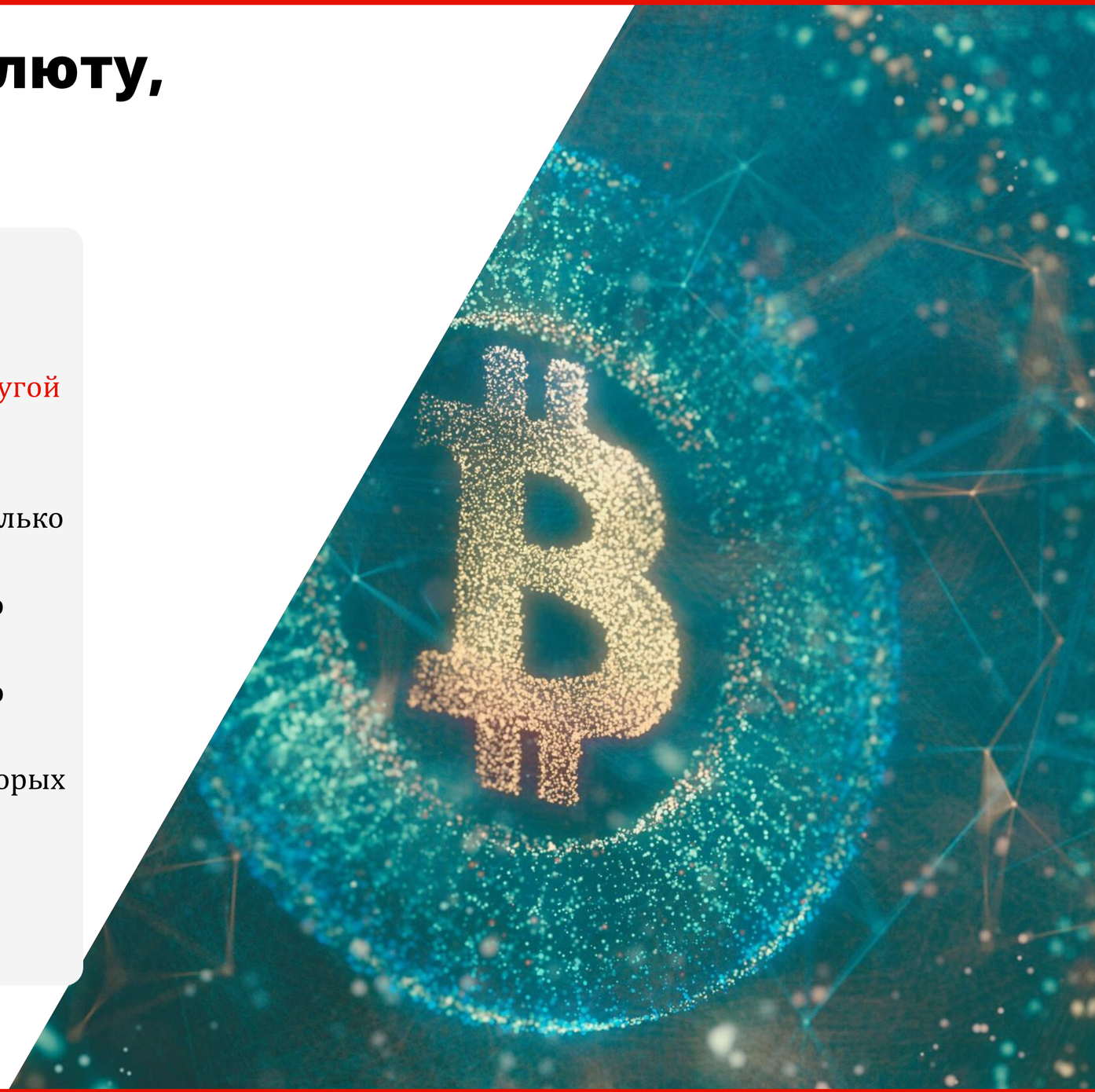
Данный вид мошенничества нацелен на сбор персональных данных и банковских сведений. Такие сайты один в один идентичны с реальными сайтами.

К примеру, Вы выложили объявление на одном из сайтов, и к Вам обращается ранее незнакомый человек и просит оформить доставку, После чего он направляет ссылку для оформления. Перейдя по ссылке, будет предложено ввести Ваши данные, то есть ФИО, год рождения, номер банковской карты, срок действия и **CVV**-код. После заполнения начинается списывание денежных средств с банковской карты.

Инвестирование в криптовалюту, ценные бумаги и т.п.

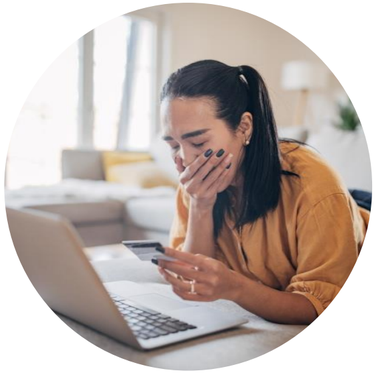
К примеру, в социальных сетях Вы увидели рекламу, где предлагается заработать на покупке и продаже акций или криптовалют. С Вами созванивается злоумышленник, представляется сотрудником Национальной компании либо другой организации, якобы предоставляющей услуги брокеров. Заманивают выгодными предложениями, уговаривают внести денежные средства, для начала небольшие суммы. Через несколько дней возвращают вложенные денежные средства с якобы заработанной выгодой. После чего просят внести уже суммы по значительней.

Многие из тех, кто попался на уловки мошенников говорят, что злоумышленники ведут себя уверенно, убедительно и в своем арсенале имеют хорошо разработанные интернет-сайты, в которых проходишь регистрацию, и в личном кабинете наблюдаешь за приумножением своих сбережений, но это все фейк;



ЧТО ТАКОЕ ДРОППЕР И ДРОПОВОД?

ДРОППЕР (DROPPER)

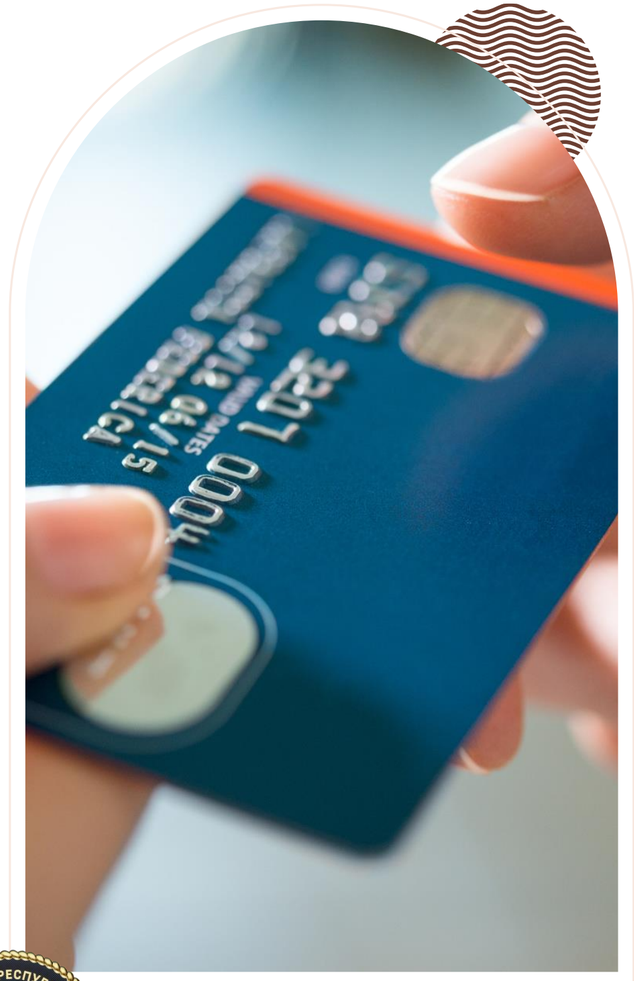


Это человек, который за определенное вознаграждение предоставляет свои личные данные, банковские счета или карты для осуществления незаконных финансовых операций. Чаще всего такие люди не подозревают, что участвуют в преступной схеме.

ДРОПОВОД (DROP HANDLER)

Дроповод **(drop handler)** — это организатор мошеннической схемы, который вербует, контролирует и использует дропперов для проведения незаконных финансовых операций.

КАК ОНИ РАБОТАЮТ?



Дропперы

- Регистрация на подставные лица: Дропперы регистрируют банковские карты и счета на свои имена.
- Передача данных: Затем они передают данные мошенникам или "кураторам", которые используют их для обналичивания украденных средств.
- Риск и ответственность: Хотя дроппер получает небольшую компенсацию, он несет наибольший риск, так как закон считает его владельцем счета.

Дропповоды

- Вербовка: Дроповоды находят людей (дропперов) через соцсети, объявления или личные контакты, обещая легкие деньги за "простую" работу.
- Инструктаж: Они обучают дропперов, как правильно открывать счета, и что делать с полученными деньгами.
- Координация и контроль: Дроповоды управляют всей схемой, распределяют роли и следят за соблюдением инструкций.
- Избежание ответственности: Обычно дроповоды остаются в тени, избегая прямого участия в финансовых операциях, что затрудняет их поимку.

Будьте на шаг впереди мошенников: Советы для безопасности

- **Чтобы не попасть на уловки мошенников которые представляются сотрудниками банков, необходимо включить функцию E-gov, где мошенники не смогут оформить онлайн кредит на Ваше имя.**
- **Проверяйте продавцов и сайты. Не спешите с покупками, всегда ищите отзывы и подтверждения надежности.**
- **Не переходите по подозрительным ссылкам. Они могут вести на фишинговые сайты.**
- **Используйте сложные пароли и двухфакторную аутентификацию. Это сделает доступ к Вашим аккаунтам более защищенным.**
- **Никогда не сообщайте данные банковских карт и пароли незнакомцам, они могут быть использованы в злоумышленнных целях.**
- **Будьте бдительны при звонках и сообщениях от "банков" и "правоохранителей". Сотрудники банка и правоохранительных органов никогда не попросят ваши личные данные**
- **Проверяйте всю информацию в интернете дважды, прежде чем верить и действовать.**

Помните: ваша безопасность в интернете зависит от вашей внимательности и осторожности.