Министерство образования Воронежской области информирует о том, что Главным следственным управлением Главного управления Министерства внутренних дел Российской Федерации по Воронежской области на постоянной основе осуществляется анализ обстоятельств, способствовавших совершению преступлений, в том числе связанных с дистанционными хищениями денежных средств граждан.

С учетом установленных правовых барьеров, ограничивающих вывод похищенных денежных средств и введения уголовной ответственности за передачу электронных средств платежа и их использование лицами, не являющимися клиентами финансово-кредитных организаций, современные злоумышленники активно пользуются услугами «курьеров».

Зачастую для выполнения роли «курьеров» под угрозами применения насилия, а также привлечения к уголовной ответственности привлекаются лица в возрасте от 18 до 25 лет, а также несовершеннолетние.

С 1 сентября 2025 года вступили в силу Федеральные законы от 31 июля 2025 г. № 281-ФЗ и № 282-ФЗ, установившие специальную административную и уголовную ответственность за нарушение требований к использованию абонентского терминала пропуска трафика и виртуальной телефонной станции (сим-боксов). Важно понимать, что уголовная ответственность по ст. 274.3 УК РФ наступает уже за сам этап организации

канала связи для совершения преступлений, то есть за незаконное использование сим-бокса.

Сим-бокс (или Sim-бокс) это специальное оборудование, которое выглядит как металлический короб с антеннами и множеством слотов для Sim-карт (иногда до нескольких десятков или даже сотен).

По своей сути это сложный программно-аппаратный комплекс, предназначенный для объединения большого количества сим-карт под единым управлением. Это устройство обеспечивает удаленный доступ к каждой из этих сим-карт, предоставляя возможность совершать телефонные звонки и рассылать текстовые сообщения неограниченному числу абонентов дистанционно.

Помимо ответственности за организацию канала связи, лицо, использующее Sim-бокс, подлежит привлечению к уголовной ответственности и за совершение мошеннических действий. Так, в случае если с использованием такого оборудования у потерпевшего (жертвы) похищены денежные средства, содеянное квалифицируется по соответствующим частям статьи 159 УК РФ (мошенничество).

Одновременно, существует отдельная статья за организацию незаконной передачи Sim-карт третьим лицам (ст. 274.4 УК РФ), по которой могут привлечь тех, кто нелегально продает сим-карты для таких Sim-боксов.

В период с 1 сентября 2025 года уголовные дела по новому составу статьи 274.3 УК РФ возбуждены в более чем в 38 субъектах Российской Федерации.

Критически важные правила безопасности необходимо донести до каждого обучающегося.

Нельзя соглашаться на предложения от незнакомцев о «легком заработке». Достаточно часто в такие схемы вовлекаются несовершеннолетние, студенты, которым предлагают небольшую заработную плату за то, чтобы они в арендованной квартире следили за работой Sim-боксов. В настоящее время такие действия навсегда могут испортить биографию и даже лишить свободы на долгие годы.

Отдельным серьезным методом воздействия на детей со стороны иностранных вербовщиков является финансовое стимулирование - выплата реальных денег или специальной игровой валюты, при чем как в качестве «подарка», так и в качестве «заработной» платы.

В интернете, в том числе в социальных сетях, для несовершеннолетних студентов буквально расставлены «ловушки», в числе которых обещание быстрого и легкого заработка.

Мошенники, с целью сокрытия следов преступления, для завладения денежными средства потерпевших, а также переводов денежных средств, добытых преступным путем, часто используют карты открытые на третьих лиц. Конечно же, эту карту нужно попросить кого-то оформить. Для этого привлекают лиц «дропов».

Более 60% «дропов» сейчас младше 24 лет, а многие становятся ими уже с 14 лет с момента получения паспорта.

«Дропами» выступают чаще всего молодые люди, асоциальные личности, а также лица с низким уровнем правовой и цифровой грамотности. Ввиду своей неопытности для этих целей используются и несовершеннолетние. Их привлекают знакомые. «Дропов» подыскивают в учебных заведениях, особенно средне-профессионального образования, школах.

«Дропов» привлекает легкий заработок. Они чаще всего продают свои карты, не осознавая последствий. Вместе с тем на эти карты, которые находятся под управлением преступников, переводятся денежные средства, добытые преступным путем. Часто данные карты блокируются банками на основании Федерального закона № 115- ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма», а также Федерального закона № 161-ФЗ «О национальной платежной системе».

В целях ликвидации каналов вывода похищенных денежных средств с использованием так называемых «дропов», передающих злоумышленникам за денежное вознаграждение свои банковские карты и счета, Президентом

Российской Федерации подписан Федеральный закон от 24 июня 2025 года № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации», которым введена уголовная ответственность для «дропов» (указанным Федеральным законом установлен прямой запрет на передачу своих платежных данных злоумышленникам и участие в операциях с похищенными и средствами).

Если ребенок участвовал в проведении операций по так называемому «обналу», либо передал свою банковскую карту кому-либо, то необходимо обратиться в полицию. Необходимо помнить, что в целях побуждения лиц («дропов»), совершивших преступные деяния, к сотрудничеству с правоохранительными органами, а также для установления лиц, причастных к организации деятельности по осуществлению неправомерных операций с использованием электронного средства платежа («дроповодов»), в пункте 4 примечаний к статье 187 УК введено специальное основание для освобождения от уголовной ответственности.

До каждого студента необходимо донести следующую информацию:

1. Не добавлять в социальных сетях незнакомых в друзья.
2. Никому не сообщать личную информацию о себе и своих родителях, такую как номер телефона, номер банковской карты, адрес или номер школы.
3. Не скачивать программы с сомнительных сайтов и не переходить по подозрительным ссылкам.
4. Любое предложение установить программу для удаленного доступа (AnyDesk, TeamViewer и другие) — это 100% мошенничество.
5. Ничего не оплачивать в интернете без помощи родителей или близких взрослых.
6. Придумывать сложные пароли для разных сервисов и везде включать двухфакторную аутентификацию.
7. Личный профиль в социальных сетях лучше сделать закрытым, ограничив круг подписчиков и видимость постов.

8. Не публиковать лишних персональных данных (к примеру теги школы, в которой вы учитесь или фотографии с одноклассниками, отписываться от ненужных рассылок и удалять старые аккаунты, что поможет уменьшить ваш «цифровой след».

9. Тоже самое необходимо предпринять в отношении публичных высказываний, например, комментариев или отзывов.

10. Не соглашаться на личные встречи с Интернет-друзьями. Немедленно прекратить все контакты в сети, если Вам задают вопросы личного характера или интимного содержания. О подобных предложениях необходимо немедленно рассказать родителям.

11. Не верить сообщениям о крупных выигрышах, срочных проблемах у родственников или легком заработке. Любой подозрительный звонок или сообщение - повод немедленно положить трубку и рассказать родителям.

14. Не спешить переводить деньги незнакомцам. Даже если предложение очень выгодное.

15. Изучить основы цифровой безопасности и правила поведения в Интернете. Сваттинг, Доксинг, Кибербуллинг, Лжеминирование — это не шутки, это наказуемые деяния.

Студент должен четко знать, что сотрудники МВД и ФСБ никогда по телефону не предлагают принять участие в операциях по задержанию преступников. Любые операции, связанные с электронным дневником, проводятся через официальные платформы школ или портал «Госуслуги» без привлечения сторонних лиц. Представители учебных заведений, банков, операторов связи или правоохранительных органов никогда не запрашивают коды из СМС, пароли или паспортные данные по телефону.

В этой связи, повышение финансовой грамотности и осведомленности обучающихся о кибербезопасности является одной из основных задач образовательной организации.