МВД России

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по КРАСНОЯРСКОМУ КРАЮ
(ГУ МВД России по Красноярскому краю)

ул. Дзержинского, 18, Красноярск, 660017

И.о. Министра образования и науки Красноярского края

Гридасовой Т.А.

20.04.25 № 4/3703

О мерах по предупреждению преступлений, совершенных с использованием информационных технологий

Министерство образования
Красноярского края
Входящий № 75-06211
«11» 04 2025 г.

Уважаемая Татьяна Алексеевна!

Анализ криминогенной обстановки на территории Красноярского края свидетельствует о значительном числе хищений денежных средств граждан, совершенных с использованием информационно-телекоммуникационных технологий[1]. В 2024 году зарегистрировано 18 055 таких преступлений, в текущем году 3 826. По итогам прошлого года в отношении несовершеннолетних обвиняемых в суд направлено 88 уголовных дела, за 2 месяца т.г. – 11, в последнее время отмечается рост преступности среди несовершеннолетних в сфере информационных технологий.

Исходя из территориальных особенностей, в Красноярском крае более 50 % таких преступлений совершается на территории краевого центра, а также на территории г.г. Норильск, Назарово, Канск, Минусинск, Ачинск и Железногорск.

В результате анализа способов совершения преступлений, совершенных с использованием ИТТ, установлено, что в последнее время на теневом рынке активно получают доступ к аккаунтам в Telegram. Злоумышленников интересуют аккаунты как вновь зарегистрированные, так и похищенные у граждан. Чаще всего такой способ «легкого заработка» выбирают несовершеннолетние и молодежь, не осознавая потенциальных последствий. Основными целями злоумышленников являются:

- финансовые мошенничества и обман подписчиков. *Если у аккаунта есть каналы с подписчиками или контакты, злоумышленники могут от его имени предлагать вложения, «быстрые деньги», поддельные инвестиционные схемы. Взломанные аккаунты часто используются для рассылки фишинговых ссылок, после чего мошенники получают доступ к банковским картам пользователей;*

[1] Далее: ИТТ.

- политическое влияние и манипуляции. *Telegram используется, как информационная площадка, и злоумышленники могут распространять фейковые новости, осуществлять политическую пропаганду в целях дестабилизации обстановки. Подконтрольные аккаунты становятся инструментом в информационных войнах, используются для распространения радикальных идей и массовых манипуляций.*

- атаки на инфраструктуру и киберпреступления. *Используя массово скупленные аккаунты, злоумышленники могут получать доступ к администрированию Telegram-групп и каналов, рассылать спам и вирусы. Эти аккаунты также могут использоваться для DDOS-атак (попытки злоумышленников ограничить доступ пользователей к сайту, сервер или сети) на онлайн-сервисы и распространения вредоносного программного обеспечения.*

Социальные сети являются самым эффективным и широким по охвату инструментом, с помощью которого злоумышленники могут вербовать пользователей в преступные организации. Деструктивные сообщества могут нанести непоправимый вред психическому и физическому здоровью, сформировать нетрадиционные духовно-нравственные ценности, опасные взгляды и убеждения, основанные на насилии и мизантропии.

Вероятность совершения преступных посягательств и тяжесть их негативных последствий могут быть существенно снижены в результате повышения эффективности использования совместных комплексных мероприятий по предупреждению указанных преступлений.

В связи с изложенным, в целях повышения правосознания населения предлагаю довести указанную информацию до сведения подчиненных Вам сотрудников. Кроме того, в рамках реализации комплекса мероприятий, направленных на повышение эффективности деятельности по предупреждению и пресечению дистанционных хищений, предлагаем Вам направить в подведомственные учреждения профилактический материал с целью дальнейшего информирования о мерах безопасности и повышения финансовой грамотности несовершеннолетних и их родителей.

О рассмотрении настоящего информационного письма и принятых мерах прошу проинформировать Главное следственное управление ГУ МВД России по Красноярскому краю.

Приложение: профилактические материалы в формате WinRAR 3,56 Мб, правила кибербезопасности для родителей на 3 л. на адрес электронной почты: mon@krao.ru.

Заместитель начальника –
Начальник Главного следственного управления Р.А. Северин

исп.: Осауленко Т.А.
тел.: 249-94-06
8-923-327-97-57

ПРАВИЛА КИБЕРБЕЗОПАСНОСТИ ДЛЯ РОДИТЕЛЕЙ

Учитывая, что инновационные технологии все больше входят в повседневною жизнь человека, в настоящее время появилась потребность формирования навыков обеспечения безопасного обращения с персональными данными и сознательного распоряжения виртуальными ресурсами с раннего возраста. Подобные социальные навыки необходимо фактически доводить до состояния безоговорочной психологической аксиомы.

Для детей в возрасте от 5 до 7 лет

- не допускать бесконтрольного времяпрепровождения в «Интернете», особенно используя гаджеты взрослых, на которых установлены программы дистанционного банковского обслуживания, приложения операторов связи, а также ФГИС «Единый портал государственных и муниципальных услуг (функций)» или исключить доступ к ним вовсе;
- не позволять детям осуществлять переходы по ссылкам самостоятельно, без контроля взрослых;
- обеспечить для нужд ребенка установку поисковых систем с возможностью установления функции родительского контроля, на которой обеспечить своевременное выставление возрастных ограничений;
- ограничить количество времени, проводимого детьми в сети «Интернет»;
- разъяснить детям о запрете на разглашение кому-либо в сети «Интернет» сведений о себе или своей семье.

Для детей в возрасте от 8 до 10 лет

- знать, чем ребенок увлекается в сети «Интернет»;
- разъяснять об опасностях, скрывающих в сети «Интернет»;
- объяснить, в чем опасность распространения в сети «Интернет» персональных данных;
- рассказать о правилах общения с друзьями посредством сети «Интернет», напомнить о том, что по ту сторону экрана всегда незнакомец;
- прислушиваться к детям, когда они пытаются донести, что при общении в сети «Интернет» столкнулись с информацией, вызывающей страх, неловкость и дискомфорт;
- обеспечить ребенку возможность использовать электронную почту, к аккаунту которой у взрослого есть доступ.

Для детей в возрасте от 11 до 13 лет

- не размещать устройства, подключенные к «Интернету», в детских

комнатах;

- установить родительский контроль на гаджетах, используемых несовершеннолетним, соответствующий возрасту ребенка;
- использовать инструменты фильтрации и мониторинга;
- обеспечить контроль всех устройств с доступом в «Интернет» (сотовые телефоны, игровые устройства, iPod и КПК);
- наладить доверительные отношения с детьми, позволяющие в любой момент получить от них сведения об их действиях в сети и людях, с которыми они общаются;
- запретить детям разглашать личную информацию без разрешения законного представителя;
- разъяснить, что не следует организовывать личные встречи с людьми, с которыми они познакомились в «Интернете»;
- иметь доступ к электронной почте и чатам детей;
- ограничить общение посредством мгновенных сообщений списком друзей, которых законные представители одобрят;
- блокировать доступ к чатам с сомнительным содержанием;
- довести детям о неэтичном поведении в интернете, в том числе о буллинге (травле), распространении сплетен, угрозах, ненормативной лексике и прочих неприятностях;
- осуществлять проверку истории браузера, чтобы отслеживать поведение детей в интернете;
- соблюдать минимальный возраст для регистрации в социальных сетях (например, 13 лет для Myspace и Facebook);
- поощрять посещение детьми соответствующих возрасту сайтов, таких как TweenLand, ClubPenguin и прочих;
- не позволять детям публиковать фотографии или видео без разрешения законного представителя.

Для детей в возрасте от 14 до 18 лет

- составить список правил использования сети «Интернет» для дома;
- установить родительский контроль, соответствующий возрасту ребенка;
- использовать инструменты фильтрации и мониторинга;
- ознакамливаться на регулярной основе с приложениями для обмена сообщениями, которые используют дети;
- обсуждать с подростками их друзей, с которыми они познакомились в сети «Интернет», и говорить об их действиях в сети;
- поговорить с подростками о том, что не следует общаться с незнакомцами посредством мгновенных сообщений, и необходимо совместно составить список их друзей;
- убедить подростков спрашивать одобрения у законных представителей, прежде чем заводить знакомства в сети;

- сопровождать подростка на встречу с людьми, с которыми они познакомились в сети «Интернете», но еще не знают лично;
- научить подростков не разглашать личную информацию, в том числе адрес электронной почты в сети «Интернете» и отвечать на нежелательную почту;
- рассказать подросткам о законах об авторском праве и ответственном поведении в «Интернете»;
- отслеживать все финансовые операции, совершаемые подростками в «Интернете», в том числе заказ, покупку или продажу товаров;
- убедить подростков в необходимости рассказывать о неприемлемых материалах или нежелательных комментариях сексуального характера, которые они получили в интернете;
- проверять историю браузера, чтобы знать, какие сайты он посещал.

Самый главный аспект - быть с детьми в доверительных отношениях, самое главное правило - «По ту сторону экрана или звонка, всегда незнакомец!!!».

Главное следственное управление
ГУ МВД России по Красноярскому краю