УВД по ЮАО ГУ МВД России по г. Москве
ОТДЕЛ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО РАЙОНУ ЗЯБЛИКОВО ГОРОДА МОСКВЫ
(ОМВД России по району Зябликово г. Москвы)

ул. Мусы Джалиля ул., 5-6, Москва, 115580
тел. 342-71-02
03.03.2025 № 04/42-1046

Директорам ГБОУ школа № 2116, 534, 1552, 1569, 991, ОЧУ СОШ «Классика», ГБПОУ ОКГ «Столица», Московский филиал ФГБОУ высшего образования «Высшая Школа народных искусств (академия)»

Уважаемые руководители!

Направляем в Ваш адрес методические рекомендации и памятки по предупреждению вовлечения молодежи и несовершеннолетних лиц в преступную деятельность, связанную с использованием информационно-коммуникационных технологий для изучения, использования в практической деятельности.

С целью профилактики мошеннических действий, повышения общего уровня информированности учащихся и их родителей необходимо разместить указанную информацию на Интернет-ресурсах образовательного учреждения, в том числе в классных и школьных чатах.

Приложение:
1.Памятка_для_родителей.
2. Памятка_для_родителей2
3. Памятка по дист. мошенничествам
4. Памятка

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 6DDD905CDB65B14F792B72FC036AC544
Владелец **Ильясов Ильгиз Мансурович**
Действителен с 04.06.2024 по 28.08.2025

Начальник ОМВД России
по району Зябликово г. Москвы
полковник полиции И.М. Ильясов

исп. Бородич Д.Н.

Памятка для родителей
по предупреждению вовлечения несовершеннолетних в преступную деятельность с использованием информационно-коммуникационных технологий

В последнее время участились случаи хищения денежных средств с банковских счетов путем обмана несовершеннолетних абонентов мобильных операторов и пользователей сетей

Основные способы совершения мошенничеств в отношении детей:

Мошенники представляются сотовыми операторами или сотрудниками «Госуслуг»	Несовершеннолетним звонят неизвестные лица и представляются сотрудниками сотового оператора и сообщают о необходимости закрепления за ними телефонного номера, под предлогом наложения на денежные средства и драгоценные металлы родителей, убеждают детей прислать фотографию банковской карты родителей, либо других взрослых лиц (бабушки, дедушки и т.д.) и сообщить код, направленный на телефон, привязанный к карте, или убеждают взять телефон родителей и осуществить переводы на счета мошенников
	Через соцсети или мобильный телефон злоумышленники связываются с детьми и говорят о том, что у родителей заблокирован сайт «Госуслги», для разблокировки необходимо взять мобильный телефон одного из родителей, уйти из дома, на телефонные звонки не отвечать, далее убеждают их через мобильное приложение банка осуществить переводы на счета мошенников с телефона родителей
Мошенники представляются сотрудниками правоохранительных органов	Неустановленное лицо осуществляет звонок несовершеннолетнему, представляется сотрудником правоохранительных органов и под предлогом декларирования денежных средств, оказывая психологическое давление в виде угроз (привлечение родителей к уголовной ответственности, помещение несовершеннолетнего в детский дом), просит провести обыск в квартире, после чего все найденные денежные средства упаковать и передать неизвестным лицам
Еще один криминальный тренд – хищение средств у детей под предлогом получения различных внутриигровых предметов в сфере электронных игр	Дети, желая получить валюту, улучшенного персонажа или артефакта в онлай-игре, сами того не понимая, предоставляют мошенникам удаленный доступ к телефону одного из родителей, для этого мошенники уверяют детей прислать фотографию банковской карты и сообщить код из СМС, который пришел на телефон родителей или же просят логин и пароль от личного кабинета маркетплейса, например OZON, Wildberiess
Мошенники втяивают детей «сверхприбыльные проекты»	Злоумышленники устанавливают с подростком контакт и предлагают быстро заработать, делая букмекерские ставки на своих ресурсах. Системы визуально показывают якобы успешность такой деятельности ребенка. Для вывода «заработка» они просят оплатить комиссию. В итоге деньги вместе с данными карты оказываются в руках киберпреступников.
	От мошенников могут поступать указания: съездить на определенный адрес с целью забрать денежные средсва, за что подросток получит денежное вознаграждение. В этом случае ребенок становится соучастником преступления.

Как обеспечить безопасность детей в сети Интернет

Для недопущения вовлечения несовершеннолетних в противоправную деятельность рекомендуется:

1. **Проверять переписку в социальных сетях** («Вконтакте», «Одноклассники», «Twitter», «Facebook» и т.п.) **и мессенджерах** (WhatsApp, Telegram, Signal, Wickr Me), на предмет наличия противоправного контента, а также наличия второго аккаунта.
2. **Проверять истории браузера**.
3. Проверять установленные **платежные системы** и транзакции, которые осуществляются с их помощью,
4. Подключить функцию «**Родительский контроль**» на телефоне Вашего ребенка. Данная функция предназначена для того, чтобы оградить Вашего ребенка от противоправного контента, расположенного в открытом доступе в сети Интернет.

В целях предупреждения дистанционных мошенничеств и краж в отношении вас и ваших детей убедительно просим провести со своими детьми разъяснительные беседы о соблюдении простых рекомендаций, которые помогут вам сохранить денежные средства и ценности:

не сообщать посторонним лицам реквизиты банковских карт, код из СМС или push-уведомлений;

не разговаривать по телефону или через мессенджеры с незнакомыми людьми;

сохранять приватность: в социальных сетях и мессенджерах нельзя раскрывать личную информацию, например, домашний или школьный адрес, имена и номера телефонов родителей, а также отмечать места, где они часто бывают;

не встречаться с незнакомыми людьми из интернета без ведома родителей;

не сообщать логины, пароли и другую конфиденциальную информацию;

отключать возможность оплаты привязанной к аккаунту картой, если ребенок имеет доступ к смартфону или компьютеру родителей;

установить на устройство ребенка защитное решение – оно не позволит перейти по фишинговой и скам-ссылке, в том числе по тем, что могут скрываться за QR-кодами или распространяться в мессенджерах и соцтетях;

погрузитесь в онлайн-мир ребенка, проявите интерес к тому, что он делает, какие сайты посещает, какие видео смотрит;

установите ПИН-код на сим карту устройства, чтобы предотвратить ее использование на других устройствах.

Помните: Если ВЫ или ВАШИ близкие стали жертвами мошенников, или ВЫ подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обратитесь в полицию! ЗВОНИТЕ «02», «102» Вам обязательно помогут!

ГУ МВД России по г. Москве

Памятка для родителей
по обнаружению нежелательного контента
на мобильных устройствах несовершеннолетних

В последнее время участились случаи хищения денежных средств с банковских счетов путем обмана несовершеннолетних абонентов мобильных операторов и пользователей сетей

Как обеспечить безопасность детей в сети Интернет

Рекомендации, которые следует принять во внимание:

поговорите со своими детьми о друзьях, с которыми они общаются в он-лайне, узнайте, как они проводят досуг и чем увлекаются;

интересуйтесь какие веб сайты посещают ваши дети и с кем разговаривают;

настаивайте на том, чтобы ваши дети никогда не соглашались встречаться со своим он-лайновым другом без Вашего ведома;

научите своих детей никогда не предоставлять личную информацию о себе и своей семье электронной почте и в разных регистрационных формах, предлагаемых владельцами сайтов;

контролируйте информацию, которую загружает ребенок (фильмы, музыку, игры и т.д.);

убедитесь, что дети консультируются с Вами, относительно любых финансовых операциях, осуществляя заказ, покупку или продажу через Интернет Сеть;

информируйте детей относительно потенциального риска при их участии в любых играх и развлечениях.

Для недопущения вовлечения несовершеннолетних в противоправную деятельность рекомендуется:

1. **Проверять переписку в социальных сетях** («Вконтакте», «Одноклассники», «Twitter», «Facebook» и т.п.) **и мессенджерах** (WhatsApp, Telegram, Signal, Wickr Me), на предмет наличия противоправного контента, а также наличия второго аккаунта.
2. **Проверять истории браузера**.
3. Проверять установленные **платежные системы** и транзакции, которые осуществляются с их помощью,
4. Подключить функцию «**Родительский контроль**» на телефоне Вашего ребенка. Данная функция предназначена для того, чтобы оградить Вашего ребенка от противоправного контента, расположенного в открытом доступе в сети Интернет.

В целях предупреждения дистанционных мошенничеств и краж в отношении вас и ваших детей убедительно просим провести со своими детьми

разъяснительные беседы о соблюдении простых рекомендаций, которые помогут вам сохранить денежные средства и ценности:

не сообщать посторонним лицам реквизиты банковских карт, код из СМС или push-уведомлений;

не разговаривать по телефону или через мессенджеры с незнакомыми людьми;

сохранять приватность: в социальных сетях и мессенджерах нельзя раскрывать личную информацию, например, домашний или школьный адрес, имена и номера телефонов родителей, а также отмечать места, где они часто бывают;

не встречаться с незнакомыми людьми из интернета без ведома родителей;

не сообщать логины, пароли и другую конфиденциальную информацию;

отключать возможность оплаты привязанной к аккаунту картой, если ребенок имеет доступ к смартфону или компьютеру родителей;

установить на устройство ребенка защитное решение – оно не позволит перейти по фишинговой и скам-ссылке, в том числе по тем, что могут скрываться за QR-кодами или распространяться в мессенджерах и соцтетях;

погрузитесь в онлайн-мир ребенка, проявите интерес к тому, что он делает, какие сайты посещает, какие видео смотрит;

установите ПИН-код на сим карту устройства, чтобы предотвратить ее использование на других устройствах.

Помните: Если ВЫ или ВАШИ близкие стали жертвами мошенников, или ВЫ подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обратитесь в полицию! ЗВОНИТЕ «112» Вам обязательно помогут!

УОДУУПиПДН ГУ МВД России по г. Москве

ОСТОРОЖНО! ТЕЛЕФОННЫЕ МОШЕННИКИ

Мошенник может представиться:
- сотрудником банка;
- сотовым оператором или сотрудником «Госуслуг»;
- сотрудником полиции или иного ведомства правоохранительной направленности;
- сотрудником Росфинмониторингга и т.д.;
- родственником

И назвать причину звонка:
- ваша карта заблокирована;
- в отношении вашей карты предпринимаются мошеннический действия;
- необходимо задекларировать денежные средства, ювелирные изделия и иные ценности;
- вашему родственнику нужна помощь

Мошенник может попросить:

Данные карты:
- номер карты;
- CVV/CVC-код;
- PIN-код;
- срок действия карты.

Пароль:
- из интернет-банка;
- из SMS-сообщения.

Перевести деньги:
- на специальный счет или карту, где они будут в безопасности, либо передать курьеру

НЕ

- сообщайте никому данные карты;
- сообщайте никому пароли и коды из SMS;
- выполняйте действия с банковской картой по просьбе третьих лиц;
- не вступайте в диалог с неизвестными лицами.

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ! ЗВОНИТЕ «02» ИЛИ «112»
ВАМ ОБЯЗАТЕЛЬНО ПОМОГУТ!

ОСТОРОЖНО! МОШЕННИКИ!

признаки мошенничества

Давление: **«Если не сделаешь это сейчас, будет хуже»**

Срочность: **«Нужно прямо сейчас отправить деньги/сообщить данные»**

Угрозы: **«Твои родители могут пострадать, а тебя отправят в детский дом»**

! ОСТАНОВИСЬ!

- не отвечай **на звонки с незнакомых абонентских номеров;**

- не выполняй указания **неизвестных лиц, даже если они представились сотрудниками правоохранительных органов (с просьбой провести обыск в своем жилище, направленный на обнаружение денежных средств/передать денежные средства курьеру/передать личные данные и данные своих родственников);**

- сообщи взрослым **об указаниях неизвестных лиц;**

- обратись по номеру 02/102/112

ОСТОРОЖНО! МОШЕННИКИ!

ПРИМЕРЫ МОШЕННИЧЕСКИХ СХЕМ ДЛЯ ОБМАНА НЕСОВЕРШЕННОЛЕТНИХ

Неустановленное лицо осуществляет звонок несовершеннолетнему, представляется сотрудником правоохранительных органов и под предлогом декларирования денежных средств, оказывая психологическое давление в виде угроз (привлечение родителей к уголовной ответственности, помещение несовершеннолетнего в детский дом), просит провести обыск в квартире, после чего все найденные денежные средства упаковать и передать неизвестным лицам.

Неустановленное лицо звонит несовершеннолетнему, представляется сотрудником сотового оператора и сообщает о необходимости закрепления за ними телефонного номера, под предлогом наложения ареста на денежные средства и драгоценные металлы родителей, убеждают детей прислать фотографию банковской карты родителей, либо других взрослых лиц (бабушек, дедушек и т.д.) и сообщить код, направленный на телефон привязанный к карте, или убеждают взять телефон родителей и осуществить переводы на счета мошенников.

Неустановленное лицо осуществляет звонок несовершеннолетнему, представляется сотрудником «Почты России», просит сообщить SMS-код, после чего получает доступ к личному кабинету Госуслуг. Позже поступает звонок от якобы сотрудника Центрального банка, который сообщает, что он занимается данным фактом взлома, а также, что от имени несовершеннолетнего осуществлен перевод денежных средств в помощь Украине и он подозревается в совершении преступления. Далее по указаниям неизвестных лиц, под угрозой уголовной ответственности, несовершеннолетний снимает денежные средства с банковских счетов родителей, сдает найденные дома ценности в ломбард, приобретает SIM-карту и новый телефон, на котором устанавливает приложение «Мир Пей», вводит данные банковской карты, указанные неизвестным, после чего зачисляет на карту денежные средства, под предлогом их сохранения на «безопасном счете».

Еще один криминальный тренд – хищение средств у детей под предлогом получения различных внутриигровых предметов в сфере электронных игр

Мошеннические схемы в игре Roblox

Roblox – одна из самых популярных онлайн-игр среди детей и подростков. Это целая платформа, где пользователи могут создавать свои миры зарабатывать внутриигровую валюту (Robux) и взаимодействовать с другими игроками. Однако на волне популярности Roblox активизировались мошенники, которые находят новые способы обмана.

Мошенник предлагает купить игровую валюту вне официального магазина по заниженной цене

Для «оплаты» просит данные банковской карты или платежных средств родителей

После перевода денег ничего не отправляет или получает доступ к карте для дальнейших списаний

ВАЖНО!

Любые онлайн-видеоигры требуют осторожности, так как в них всегда есть риски столкнуться с деструктивным поведением, например буллингом, или мошенничеством.

Для защиты от злоумышленников мы рекомендуем:

- Исключить «привязку» платежных средств к игровым аккаунтам;
- Ограничить доступ детей к платежным средствам родителей;
- Обсудить с ребенком важность кибербезопасности. Объяснить, что даже в игре нельзя передавать личные данные, пароли и платежные реквизиты.

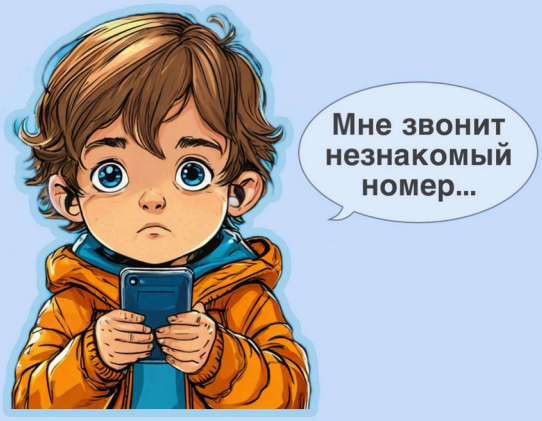
ОСТОРОЖНО! МОШЕННИКИ!

ПРИЗНАКИ МОШЕННИЧЕСТВА:

Давление: «Если не сделаешь это сейчас, будет хуже»

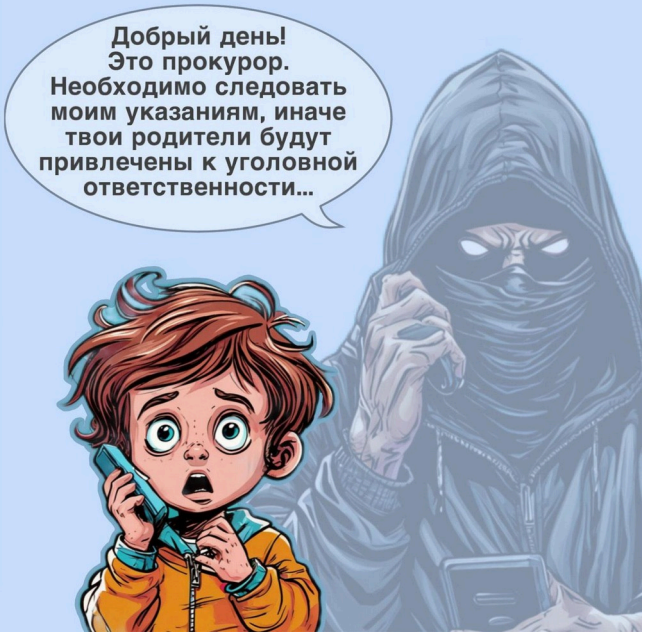
Срочность: «Нужно прямо сейчас отправить деньги/сообщить данные»

Угрозы: «Твои родители могут пострадать, а тебя отправят в детский дом»



⚠ ОСТАНОВИСЬ! ⚠

- **не отвечай** на звонки с незнакомых абонентских номеров;
- **не выполняй указания** неизвестных лиц, даже если они представились сотрудниками правоохранительных органов (с просьбой провести обыск в своем жилище, направленный на обнаружение денежных средств/ передать денежные средства курьеру/ передать личные данные и данные своих родственников);
- **сообщи взрослым** об указаниях неизвестных лиц;
- обратись по номеру **02/102/112.**



ПРИМЕРЫ МОШЕННИЧЕСКИХ СХЕМ ДЛЯ ОБМАНА НЕСОВЕРШЕННОЛЕТНИХ

ОСТОРОЖНО! МОШЕННИКИ!

!

Неустановленное лицо осуществляет звонок несовершеннолетнему, представляется сотрудником правоохранительных органов и под предлогом декларирования денежных средств, оказывая психологическое давление в виде угроз (привлечение родителей к уголовной ответственности, помещение несовершеннолетнего в детский дом), просит провести обыск в квартире, после чего все найденные денежные средства упаковать и передать неизвестным лицам.

!

Неустановленное лицо осуществляет звонок несовершеннолетнему, представляется сотрудником государственной организации и под предлогом замены полиса ОМС, просит сообщить SMS-код, после чего получает доступ к личному кабинету Госуслуг. Позже поступает звонок от якобы сотрудника «Росфинмониторинга», который предупреждает, что во избежание совершения мошенничества, необходимо провести видео-обыск в квартире на наличие ценностей посредством мессенджера «Telegram» и никому об этом не сообщать. В случае отсутствия доступа к ценностям, находящимся в сейфе, неизвестное лицо под видом специалиста лично приезжает в квартиру и вскрывает сейф. Получив доступ ко всем ценностям, несовершеннолетний передает их неизвестным лицам под угрозой возникновения у родителей проблем, связанных со спонсированием терроризма.

!

Неустановленное лицо осуществляет звонок несовершеннолетнему, представляется сотрудником «Почты России», просит сообщить SMS-код, после чего получает доступ к личному кабинету Госуслуг. Позже поступает звонок от якобы сотрудника Центрального Банка, который сообщает, что он занимается данным фактом взлома, а также, что от имени несовершеннолетнего осуществлен перевод денежных средств в помощь Украине и он подозревается в совершении преступления. Далее по указаниям неизвестных лиц, под угрозой уголовной ответственности, несовершеннолетний снимает денежные средства со своих банковских счетов, сдает найденные дома ценности в ломбард, приобретает SIM-карту и новый телефон, на котором устанавливает приложение «Мир Пей», вводит данные банковской карты, указанные неизвестным, после чего зачисляет на карту денежные средства, под предлогом их сохранения на «безопасном счете». Также сообщают, что в квартире будет проводится обыск, во время проведения которого несовершеннолетнему необходимо переночевать в другой квартире, арендованной неизвестными лицами.