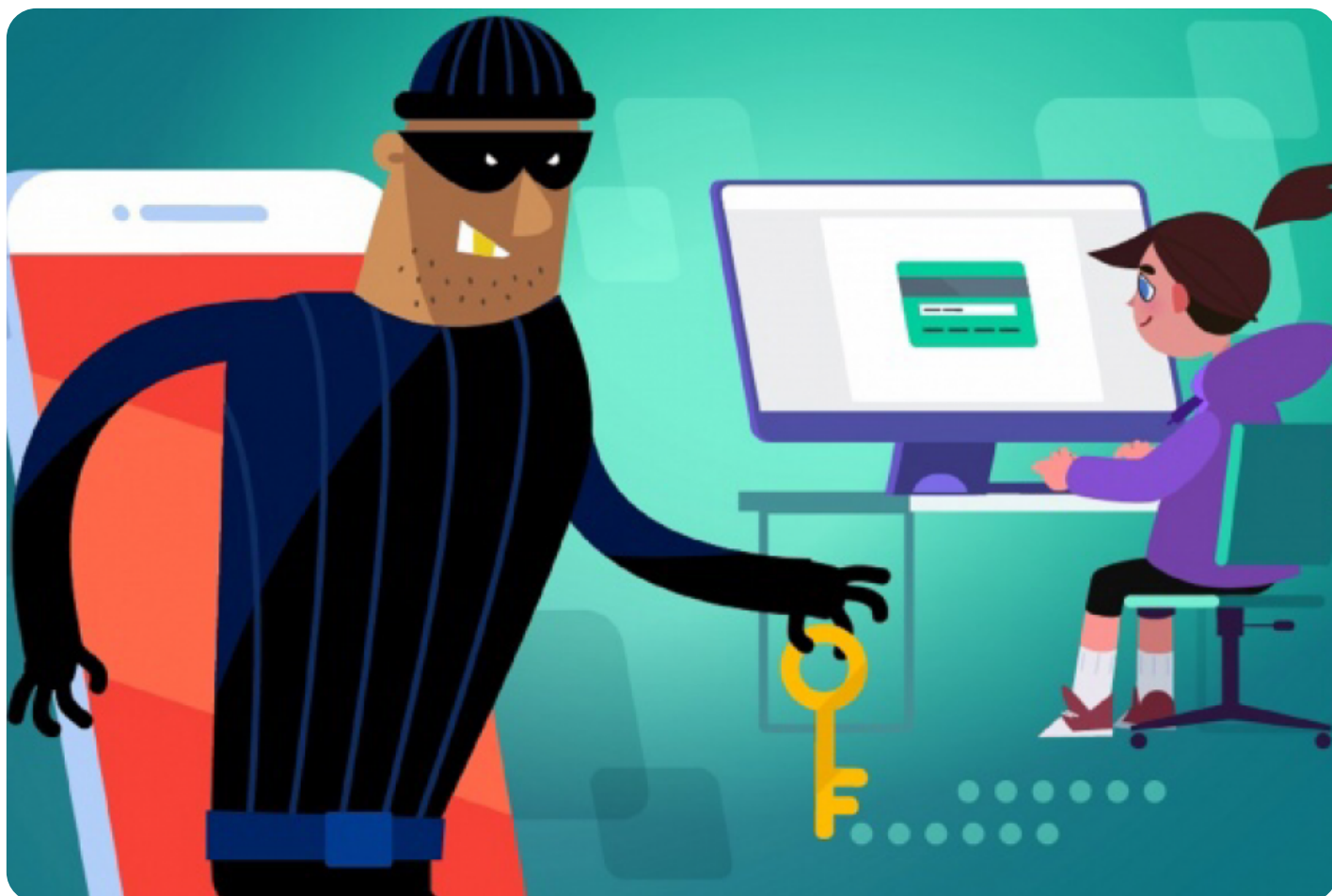




**УПРАВЛЕНИЕ
ОБРАЗОВАНИЯ**
Администрации ГО г. Уфа РБ

СПОСОБЫ ЗАЩИТЫ ДЕТЕЙ

ОТ КИБЕРМОШЕННИЧЕСТВА



АЛГОРИТМЫ РАЗЪЯСНЕНИЯ РОДИТЕЛЯМ СПОСОБОВ ЗАЩИТЫ ДЕТЕЙ ОТ КИБЕР- МОШЕННИЧЕСТВА

Бдительность при общении онлайн

1

- научите ребенка не делиться личной информацией, такой как адрес, номер телефона, пароли или данные банковских карт с незнакомыми людьми;
- не позволяйте детям открывать ссылки из сомнительных источников и загружать файлы от неизвестных отправителей.

Надежные пароли и двухфакторная аутентификация

2

- обеспечьте защиту личных аккаунтов;
- установите двухфакторную аутентификацию (2FA) на игровых и социальных платформах.

Обучение финансовой грамотности

3

- проводите беседы с детьми о деньгах, как работают финансовые операции;
- разъясняйте, как работают банковские карты, что такое мошенничество и как его можно избежать;
- запретите детям сообщать PIN-коды, запрашивать данные на пластиковых картах и проверять выписки по счетам.

Настройка приватности в социальных сетях

4

- запретите детям публиковать личные данные, такие как местоположение, фотографии, на которых видны дом или школа, и другую информацию, которая может привлечь мошенников;
- научите детей использовать настройки приватности.

Онлайн-покупки

5

- научите детей пользоваться только проверенными платформами и сайтами интернет-магазинов;
- выбирать опции с защитой покупок, а также следите за выписками по картам на предмет неожиданных транзакций;
- научите ребенка обращать внимание на адекватность цен.

Регулярные проверки компьютеров и мобильных устройств

6

- установите антивирусные программы для защиты от вредоносного программного обеспечения;
- установите запрет на установку программ или приложений без предварительной проверки и обсуждения с родителями.

Открытое общение о рисках

7

- проводите постоянные беседы с детьми о рисках, связанных с интернетом;
- установите с ребенком доверительные отношения, чтобы дети знали, что могут поделиться с вами своими подозрениями и переживаниями;
- обсуждайте вместе новости о мошенниках и делитесь актуальными примерами, чтобы ребенку стало легче воспринимать информацию.

ОСНОВНЫЕ СПОСОБЫ МОШЕННИЧЕСТВА

СМС от различных сервисов (Госуслуги, банки, операторы связи, социальные сети и т.п.) о взломах аккаунтов.

– **МОЖЕТ ПОСТУПИТЬ СООБЩЕНИЕ** о взломе аккаунта, страницы с указанием номеров телефона/ ссылок на страницы сайтов, по которым нужно обратиться/ перейти для решения возникшей проблемы;

– **ПОСЛЕ ПОЛУЧЕНИЯ СМС ПОСТУПАЕТ ЗВОНОК** от неизвестного лица (либо пользователь сам перезванивает по указанному номеру телефона/переходит по ссылке), которое представляется специалистом сервиса и предлагает помощь в решении проблемы (восстановить аккаунт, обеспечить безопасность персональных данных и т.д.), предупреждает о возможном мошенничестве со стороны третьих лиц, в результате которого произошел взлом, может сообщить, что с тобой свяжется в ближайшее время сотрудник правоохранительных органов (МВД, Следственный комитет, ФСБ, прокуратура и др.) с целью поиска и привлечения мошенников к ответственности;

– **ПОСЛЕ РАЗГОВОРА** с тобой может связаться незнакомое лицо и представиться сотрудником перечисленных правоохранительных

органов и сориентировать на определенный порядок действий, который необходимо выполнять в связи с имеющейся угрозой в отношении тебя со стороны мошенников либо иных лиц (пройти по ссылкам, поступившим от него или его представителей в мессенджерах, быть с ним постоянно на связи, предоставить ему персональные данные, доступ к аккаунтам в мессенджерах, запрет на информирование родителей и близких о сложившейся с тобой ситуации, покинуть город, не возвращаться домой);

– **ПОСЛЕ ЭТОГО МОГУТ ПОСТУПИТЬ ЗВОНКИ** от этих же лиц либо от других, но тоже представляющихся сотрудниками правоохранительных органов либо банков, о попытках перевода твоих личных сбережений на иностранные счета, финансирования таким способом терроризма либо ВС Украины и т.п.), и предложениях в целях пресечения преступных операций о необходимости осуществления переводов денежных средств на «безопасные счета», на которые тебе указывают звонившие, либо получения обманным способом этих

средств от родителей и необходимости их перевода неизвестным.
Необходимость перевода денег на «безопасный счет».

– МОГУТ ПОСТУПИТЬ ЗВОНКИ ОТ НЕИЗВЕСТНЫХ ЛИЦ, которые представляются сотрудниками банков, служб безопасности, Центрального банка России либо правоохранительных органов, и сообщают о якобы совершающихся в отношении тебя мошеннических действиях (оформление кредитов, микрозаймов) и для предотвращения хищения твоих денег необходимо перевести их на «безопасный счет», после чего просят доступ к личному кабинету банка, где у тебя есть лицевые счета;

– ЗВОНКИ МОГУТ ПОСТУПАТЬ ПО НЕСКОЛЬКО ДНЕЙ ПОДРЯД либо с перерывами, так злоумышленники входят в доверие и убеждают в необходимости совершения тобой определенных действий;

– В ХОДЕ ОБЩЕНИЯ С ТОБОЙ неизвестные лица для подтверждения

своих слов и действий могут отправлять фото документов, похожих на подлинные.

Взлом либо копирование аккаунта пользователя в мессенджерах Ватсап, Вайбер, Телеграм, социальных сетей Вконтакте и т.п.

– С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТИ (искусственный интеллект) генерируются видеозвонки, голосовые сообщения от имени твоих знакомых, родственников, друзей, у которых взломаны аккаунты в мессенджерах / социальных сетях, с полностью скопированными голосом и изображением, с использованием ранее отправленных видео и аудио сообщений твоих знакомых, родственников;

– ПОСТУПАЮТ ПРОСЬБЫ ОКАЗАТЬ ФИНАНСОВУЮ ПОМОЩЬ, сообщить о возникшей проблеме, в том числе, что твой знакомый, родственник, родитель попал в серьезную беду, происшествие, после чего могут прислать фото банковской карты либо номер телефона для перевода денег.

ПОРЯДОК ДЕЙСТВИЙ (ПРАВИЛА ПОВЕДЕНИЯ)

НЕ ВЕРИТЬ НА СЛОВО лицам, звонящим с неизвестных номеров. Все поступающие тебе звонки с неизвестных номеров нужно ставить под сомнение.

СООБЩИТЬ ЗВОНЯЩЕМУ, что ты являешься несовершеннолетним и пусть все разговоры ведут с твоими родителями, после этого сразу прекратить разговор.

НЕЗАМЕДЛИТЕЛЬНО после таких звонков сообщить о них своим родителям (законным представителям), близким родственникам либо любым лицам, которым ты доверяешь, или в полицию (номер телефона любой дежурной части), **НА ЕДИНЫЙ ТЕЛЕФОН ДОВЕРИЯ (ТЕЛ. 8-800-2000-122).**

Не перезванивать по номерам телефона, указанным в сообщениях о взломах аккаунтов, не переходить по незнакомым ссылкам из этих сообщений.

Не сообщать свои персональные данные, не предоставлять им доступ к своим страницам, аккаунтам в социальных сетях.

Не производить онлайн-платежи, переводы по просьбам неизвестных.

Не верить сообщениям с неизвестных и известных номеров (сервисов) о выигрышах, способах быстрого заработка крупных сумм, с просьбами о помощи друзьям, родственникам, займе денег,

ЕСЛИ ВСЁ ЖЕ ПОВЕРИЛ, ПРОШЁЛ ПО ССЫЛКЕ, ОТВЕТИЛ НА ЗВОНОК, СООБЩИЛ СВЕДЕНИЯ О СЕБЕ

Не паниковать. Из любой ситуации, которая может казаться очень проблемной, всегда есть выход.

Незамедлительно сообщить об этом своим родителям (законным представителям), близким родственникам либо любым лицам, которым ты доверяешь, или в полицию (номер телефона любой дежурной части), на

ЕДИНЫЙ ТЕЛЕФОН ДОВЕРИЯ (ТЕЛ. 8-800-2000-122).

Заблокировать (поместить в черный список) незнакомые номера, с которых тебе звонили, поступали сообщения.

ГЛАВНОЕ! В любой сомнительной и непонятной ситуации перед совершением действий нужно обязательно посоветоваться со взрослыми знакомыми и близкими тебе людьми, которым ты доверяешь!

Всю информацию о том, как не попасть на уловки мошенников, вы можете узнать на официальном сайте МВД по Республике Башкортостан по адресу:

WWW.02.MVD.RF