Памятка по безопасному поведению детей в Интернете

Не сообщайте личную информацию, незнакомым людям.
Такую как номер телефона, кредитной карты, адрес или номер школы.

Не соглашайтесь на личные встречи с Интернет-друзьями.
О подобных предложениях немедленно расскажите родителям.

Установите сложный и уникальный пароль для каждого аккаунта.
Используйте двухфакторную аутентификацию для усиления защиты аккаунтов.

Не спешите переводить деньги незнакомцам.
Даже если предложение очень выгодное, спросите об этом родителей!

Установите на ваши устройства защитное программное обеспечение.
Антивирус поможет защитить вас от вредоносных программ.

Изучите основы цифровой безопасности и правила поведения в Интернете.
Сваттинг, Доксинг, Кибер-буллинг, Лжеминирование - это не шутки, это наказуемые деяния.

Немедленно прекращайте любые контакты в сети.
Если вам задают вопросы личного характера или интимного содержания. Расскажите об этом родителям.

Всегда сообщайте родителям.
Обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.

Мошенники используют технику SMS-бомбинга перед проведением атак на российских пользователей.

SMS-бомбинг – это вид кибератаки, при которой преступники массово отправляют сообщения на мобильный номер конкретного человека.

На телефон жертвы поступает огромное количество сообщений якобы от государственных структур, банковских учреждений, микрофинансовых организаций, онлайн-магазинов и других всевозможных онлайн-сервисов.

В самих сообщениях отображаются различные SMS-коды, подтверждения, а также ссылки для перехода на вредоносные и фишинговые сайты.

Рассчет на панику жертвы, которая способна ответить на любое SMS-сообщение.

После SMS-атаки на телефонный номер человека поступают звонки якобы от «представителей его мобильного оператора», которые заявляют о том, что сейчас техническая поддержка наблюдает массовую SMS-атаку, в связи с чем необходимо её прекратить, для чего просят подтвердить персональные данные и указать код из SMS-сообщения.

Никогда не сообщайте незнакомым лицам поступающие на ваш телефон SMS-коды, а также ваши персональные данные.

DDoS-атака: что это такое?

DDoS-атака — это распределённая атака типа «отказ в обслуживании».

Говоря простым языком, DDoS-атака это попытка злоумышленников так загрузить сервер, чтобы он просто перестал работать.

Для этого на него отправляется очень большое количество запросов.

Для сравнения: «естественный DDoS» может происходить во время сезонных распродаж, когда онлайн-магазины сталкиваются с наплывом покупателей, не справляются с нагрузкой, и в итоге сервис работает с перебоями или становится полностью недоступным.

Совершаются такие атаки не вручную — запросы автоматические и в случае с крупными атаками могут посылаться одновременно с сотен устройств.

Устройства, используемые хакерами для DDoS-атак, почти никогда не являются их собственными — обычно это компьютеры таких же жертв злоумышленников.

Под удалённым управлением организаторов атаки находятся целые сети ПК, заражённых вредоносным ПО, а количество запросов может достигать многих тысяч.

Атаки могут совершаться на сайты государственных учреждений и банков по политическим мотивам, ради кражи информации частных компаний или из-за конкуренции в бизнесе, для отвода глаз и параллельного мошенничества, вымогательства и даже ради развлечения.

Действия за DDoS-атаки квалифицируются по общим нормам о преступлениях в сфере компьютерной информации:

- ст. 272 УК РФ (Неправомерный доступ к компьютерной информации);

- ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ)».

Максимальное наказание за совершение таких преступлений — до семи лет реального лишения свободы.

Размер штрафа может доходить до 500 тыс. руб., также хакер обязан возместить причиненный ущерб, который обычно является очень существенным.

Основные правила цифровой безопасности для родителей и их детей

Контролируемый доступ

Родители должны контролировать, какие сайты посещает ребёнок, и устанавливать фильтры для блокировки нежелательного контента.

Образование и предупреждение

Важно объяснить детям о возможных рисках в интернете, безопасных сайтах и общении в сети.

Конфиденциальность

Научите ребёнка важности защиты личной информации и объясните, какую информацию нельзя выкладывать в сеть.

Самоконтроль и ответственность

Дети должны уметь правильно принимать решения о том, что безопасно делать в интернете, что нет.

Мониторинг и сопровождение

Родители должны активно участвовать в онлайн-жизни детей, беседовать о происходящем в интернете и контролировать их активность.

Цифровая гигиена — это комплекс правил и рекомендаций по безопасному использованию цифровых устройств и ресурсов.

Она включает в себя следующие аспекты:

Защита персональных данных: используйте сложные пароли, двухфакторную аутентификацию, шифрование данных и антивирусное программное обеспечение.

Безопасность в интернете: избегайте подозрительных ссылок, загрузок и вложений, обновляйте операционную систему и приложения, устанавливайте обновления безопасности.

Конфиденциальность: ограничьте доступ к личной информации, используйте приватность в социальных сетях и мессенджерах, не делитесь конфиденциальными данными без необходимости.

Сетевая этика: уважайте права других пользователей, не нарушайте авторские права и не распространяйте ложную информацию.

Финансовая безопасность: используйте надёжные пароли для онлайн-банкинга, двухфакторную аутентификацию, не сообщайте свои данные третьим лицам и регулярно обновляйте антивирусное программное обеспечение.

Физическая безопасность: храните устройства в безопасных местах, не оставляйте их без присмотра и следите за их безопасностью.

Соблюдение правил цифровой гигиены поможет вам защитить свои личные данные, финансы и частную жизнь от возможных угроз и мошенников.

По какой причине мошенники стремятся скомпрометировать учётные записи граждан на портале «Госуслуги»?

Основная цель: оформление различных кредитных продуктов в микрофинансовых организациях с помощью скомпрометированного личного кабинета пользователя.

При получении доступа к аккаунту пользователя на портале «Госуслуги» злоумышленники могут авторизоваться на сайтах различных микрофинансовых организаций.

Небольшие по размеру займы могут быть выданы даже в том случае, если произойдёт только авторизация через портал «Госуслуги», без предоставления каких-либо дополнительных данных.

Основным способом входа в личный кабинет на портале «Госуслуги» является код подтверждения из SMS-сообщения, который аферисты могут заполучить у пользователя под различными предлогами.

Повышение уровня цифровой грамотности населения и усиление мер безопасности на портале «Госуслуги» являются важными шагами для предотвращения подобных мошеннических схем.

Поменяли сим-карту — открепите номер от Госуслуг и мобильного приложения.

Киберпреступники приобретают старые сим-карты, которые уже были использованы и поступили в повторную продажу. Затем они используют эти сим-карты для восстановления доступа к учетным записям различных онлайн-сервисов.

Это может привести к утечке конфиденциальной информации, такой как паспортные данные, информация о недвижимости и автомобилях, и другие личные данные.

Как избежать многомиллионного кредита, взятого на ваше имя другим человеком?

Первым делом открепите неиспользуемый номер телефона от портала «Госуслуг», онлайн-банка и других своих аккаунтов.

Сделать это самостоятельно можно, если сим-карта, которой вы не планируете больше пользоваться, все еще установлена в вашем телефоне. Связано это с тем, что на этот номер придет код, подтверждающий ваши действия.

Сменить номер телефона достаточно просто, на портале «Госуслуги» нужно перейти в раздел «Настройки и безопасность» и нажать «Изменить» напротив прикрепленного номера телефона.

Если же сим-карты на руках у вас уже нет – потеряли или выбросили за ненадобностью, – сменить номер на портале «Госуслуг» самостоятельно не получится. Вам необходимо обратиться в МФЦ.

Будьте бдительны и предупредите родных и близких!

«**Наиболее распространёнными и опасными мошенническими схемами являются звонки, в процессе которых телефонные аферисты стараются ввести потенциальных жертв в заблуждение, называя себя представителями правоохранительных органов или Банка России**»

В ходе реализации подобных мошеннических схем возможно два варианта развития событий.

Злоумышленники могут запросить платёжные данные пользователя или другую конфиденциальную информацию, чтобы осуществить кражу денежных средств.

Аферисты начинают убеждать пользователя самостоятельно совершать различные банковские операции под различными предлогами.

В тех случаях, когда мошенник начинает провоцировать человека на самостоятельное выполнение банковской операции, они особенно подчёркивают во время общения, что не запрашивают никаких реквизитов и данных, вызывая тем самым у потенциальной жертвы дополнительное доверие.

Основой из успешных мошеннических схем является психологическая манипуляция.

Аферисты используют страх и срочность, чтобы заставить жертв принимать быстрые решения без обдумывания.

Не передавайте личные данные по телефону и проверяйте любую информацию, поступающую из подозрительных источников.

Будьте бдительны!

Фишинг — это вид интернет-мошенничества, направленный на получение доступа к конфиденциальной информации пользователей, например, таким как логины и пароли.

Мошенники отправляют электронные письма или личные сообщения от имени популярных брендов, банков или государственных органов, в которых содержатся ссылки на поддельные сайты, внешне неотличимые от настоящих (официальных).

После перехода на поддельный ресурс аферисты пытаются побудить пользователей ввести свои логин, пароль или иную конфиденциальную информацию, которые затем используют в противоправных целях.

Чтобы распознать фишинг, обратите внимание на следующие признаки:

Упоминание в записи сообщества: мошенники могут фальсифицировать группу известной радиостанции или использовать другие популярные темы.

SMS-рассылка: злоумышленники могут включить ваш номер в SMS с предложением обмена и ссылкой на страницу якобы товара.

Электронная почта: письма могут содержать информацию о взломе почты, банковском счёте, социальных сетях, уведомления от органов власти или благотворительных организаций.

Сайты: мошенники подделывают доменные имена, используют HTML-вёрстку и маскируют адрес фишингового сайта под знакомый пользователям домен.

Отсутствие SSL-сертификата: популярные сайты используют шифрование SSL для передачи данных пользователей, адрес сайта начинается на «https://».

Грамматические, орфографические и дизайнерские ошибки: крупные компании имеют профессиональных дизайнеров и корректоров, ошибки могут указывать на мошенничество.

Подозрительные платёжные формы: проверьте структуру страниц и дизайн форм, они могут отличаться от оригинального сайта.

Отсутствие пользовательских соглашений и странные контакты: убедитесь, что текст соглашений не указывает на сторонние компании и проверьте адрес контактов.

Для противодействия фишингу соблюдайте правила интернет-гигиены, используйте антивирус и инструменты защиты.

В современном мире телефонные мошенники становятся всё более изобретательными и опасными.

Они используют различные методы обмана, чтобы украсть деньги и личные данные пользователей.

Основные методы противодействия телефонным мошенникам.

Информирование и обучение

Самый эффективный метод борьбы с телефонными мошенниками — это информирование и обучение граждан.

Необходимо рассказывать людям о возможных схемах обмана и способах защиты от них. Также стоит проводить обучающие мероприятия и тренинги для сотрудников компаний и организаций, чтобы они могли распознать мошеннические звонки и предотвратить возможные убытки.

Установка антиспам-фильтров

Многие компании и организации могут установить антиспам-фильтры на свои телефоны и компьютеры, чтобы блокировать нежелательные звонки и сообщения.

Это поможет снизить количество мошеннических звонков и уменьшить вероятность попадания в ловушку мошенников.

Проверка номеров и информации

Перед тем как предоставить свои личные данные или совершить платёж, всегда проверяйте номер телефона и информацию, которую вам предоставляют.

Мошенники часто используют поддельные номера и логотипы известных компаний, поэтому будьте осторожны и внимательны.

Использование двухфакторной аутентификации

Двухфакторная аутентификация (2FA) — это дополнительный уровень защиты, который помогает предотвратить несанкционированный доступ к вашим аккаунтам и личной информации.

Многие сервисы и приложения предлагают возможность включить 2FA, что значительно усложняет работу мошенников.

Обращение в правоохранительные органы

Если вы стали жертвой телефонного мошенничества, немедленно обратитесь в правоохранительные органы.

Также можно обратиться в специальные службы поддержки, которые помогут вам вернуть украденные средства.

Противодействие телефонным мошенникам — это важная задача, которая касается каждого из нас.

Будьте бдительны и осторожны, и тогда вы сможете избежать неприятных последствий.

Что делать если на вас оформили кредит?

Запросите кредитную историю

Информация о действующих или закрытых кредитах хранится в бюро кредитных историй (БКИ).

Самый простой способ — подать заявку через госуслуги.

Ответ приходит почти сразу. Подробная инструкция есть на портале.

Напишите заявление в полицию

Чем быстрее вы это сделаете, тем больше шансов выйти на след мошенников.

Подать заявление о преступлении можно лично в любом отделении полиции.

В заявлении укажите все важные факты: какой кредит и когда на вас оформили, какая задолженность по нему числится, а главное — попытайтесь доказать, почему это точно сделали не вы.

Обратитесь в кредитную организацию

Обратиться нужно в ту организацию, где по данным БКИ за вами числится долг. Это может быть банк или МФО. Сделать это можно и до подачи заявления в полицию.

Но если приложить копию талона-уведомления из отделения, то велика вероятность, что кредитор отнесется к обращению более внимательно и как минимум не заподозрит вас в попытке обмана и уклонения от своих долговых обязательств.

Обычно после таких заявлений банки проводят внутреннюю служебную проверку. Кредитор не меньше заемщика заинтересован выявлять и пресекать факты мошенничества при оформлении кредитов.

Если после проверки банк установит, что кредит действительно получили мошенники, он может сразу аннулировать кредитный договор.

Если банк вам не помог, можно пожаловаться на его действия в Центральный банк России либо обратиться в суд

Подайте иск в суд

Соберите документы и составьте исковое заявление.

❗К нему необходимо приложить:

- кредитный договор и все приложения к нему;
- копию паспорта заемщика, которую банк делал при выдаче кредита;
- реквизиты банковского счета или карты, куда были перечислены деньги;
- кассовый ордер или распоряжение клиента о списании денег со счета.

- Также может пригодиться ФИО и должность сотрудника, который оформил на вас кредитный договор, и адрес офиса, где это произошло, — эту информацию тоже стоит запросить в банке.

Компьютерные вирусы

Вместе с удобством и доступностью информационных технологий активно развивается одна из угроз информационной безопасности — компьютерные вирусы.

Вирусы представляют собой вредоносные программы, способные нанести значительный ущерб компьютерам, сетям и данным пользователей.

Вирусы могут проникать в компьютеры через электронную почту, файлы, веб-сайты, съёмные носители информации и другие источники.

Существует множество видов компьютерных вирусов, которые можно классифицировать по различным критериям:

По способу распространения
(файловые, загрузочные, макровирусы и сетевые).
По деструктивным возможностям
(безвредными, неопасными, опасными и очень опасными).

Способы распространения компьютерных вирусов

Вирусы распространяются через различные каналы передачи информации, такие как электронная почта, файлы, веб-сайты, съёмные носители информации и другие. Наиболее распространённым способом является электронная почта, когда вирус прикрепляется к письму в виде вложения или ссылки.

Создание и распространение компьютерных вирусов является преступлением.

Статья 273 УК РФ "Создание, использование и распространение вредоносных компьютерных программ"

Виды наказания: ограничение свободы, принудительные работы или лишение свободы на срок до семи лет.

Чтобы предотвратить распространение вирусов, необходимо:

- ▶ Соблюдать правила информационной безопасности.
- ▶ Обновлять антивирусное программное обеспечение.
- ▶ Быть внимательными при работе с электронной почтой и файлами.