



Всеволожская  
городская прокуратура

## «Как пожилым людям не стать жертвой «Интернет» – мошенников?»

2023

Цифровая безопасность касается каждого пользователя, особенно пожилых людей, которые в последнее время стали главной мишенью для кибер-преступников. Прокуратура напоминает о самых распространенных видах мошеннических действий и дает рекомендации, как их предотвратить.

### 1. Онлайн-инвестиции

Многим пожилым людям при выходе на пенсию требуются дополнительные доходы или им необходима помощь в управлении своими сбережениями, поэтому аферы с онлайн-инвестициями как раз нацелены на этих людей, обещая хорошую отдачу от инвестиций пенсионеры переводят свои средства мошенникам.

Как избежать афер с онлайн-инвестициями:

- остерегайтесь обещаний получить огромную прибыль без риска;
- избегайте предложений, которые заставляют Вас принимать быстрые действия и не оставляют время на раздумья;
- проконсультируйтесь по поводу инвестиций в своем банке или у доверенного финансового советника;
- убедитесь, что рекламируемый инвестиционный фонд имеет все необходимые лицензии и регистрации.

### 2. Онлайн-знакомства

Интернет может быть отличным местом для пожилых людей, желающих найти новые знакомства или даже любовь. Круг знакомств в Интернете огромный, но в нем водится очень много мошенников. Очень часто злоумышленники создают в Интернете поддельный профиль несуществующего человека и заводят знакомства с доверчивыми людьми с той целью, чтобы обманом выманить у них деньги. Существуют целые сценарии, в которых нужно будет заплатить деньги для члена семьи, который тяжело заболел, или для покупки билета, чтобы встретиться и познакомиться лично. Многие пожилые люди становятся жертвами этой аферы, потому что они ищут общения и могут быть слишком доверчивыми.

Как избежать афер с онлайн-знакомствами:

- ищите несоответствия в профиле нового знакомого;
- будьте осторожны с теми людьми, кто пытается установить с Вами взаимоотношения;
- расскажите своей семье или друзьям о новом знакомстве, чтобы они могли проверить профиль этого человека;
- никогда не перечисляйте деньги кому-либо, с кем Вы познакомились в Интернете.

### 3. Лотерея

Пожилые люди склонны попадаться на удочку мошенников, которые говорят им, что они выиграли в лотерею. Информацию о том, что именно Вы миллионный посетитель - можно увидеть на каком-нибудь сайте, письмо с лотерейной аферой также можно получить по электронной почте. В этом случае мошенники просят сообщить им Ваши личные и банковские данные, чтобы «перевести» выигрыш на ваш счет. Вместо этого сбережения попросту будут украдены.

**Как избежать афер с лотереями:**

- помните, что Вы не можете выиграть в лотерею, если Вы в ней никогда не участвовали;
- имейте в виду, что никто не раздает деньги просто так;
- никогда не передавайте данные доступа к вашему банковскому счету через Интернет.

### 4. Поддельные лекарства по рецептам

Пожилые люди иногда выходят в Интернет, чтобы проверить лекарства, выписанные им по рецепту и найти лучшую цену, при этом они сталкиваются с мошенниками, которые предлагают им препараты дешевле того лекарства, которое прописал врач. Как правило, такие препараты могут быть запрещены или не иметь требуемых разрешений, а потому они могут представлять реальную и серьезную угрозу для здоровья.

Как избежать афер с поддельными лекарствами:

- покупайте только те лекарства, что представлены в рецепте, и только в аптеках;
- проконсультируйтесь у своего врача о выписанном лекарстве и возможных ему альтернативах;
- если Вы купили лекарства через Интернет и не получили его, сообщите об этом в полицию и в свой банк.

### 5. Техническая поддержка

Техническая поддержка мошенников начинается со всплывающего предупреждения о проблеме с компьютером. Всплывающее окно содержит номер телефона, куда можно позвонить. Поддельные сотрудники Microsoft или Apple отвечают на телефонные звонки и убеждают вас предоставить им доступ к вашему компьютеру, чтобы они могли решить проблему. Затем они либо получают доступ к вашему банку через ваш компьютер, либо запрашивают оплату за указанный «ремонт».

**Как избежать афер с технической поддержкой:**

- не становитесь жертвой тех обращений к Вам, когда говорят о том, что нужно срочно предпринять какие-то меры;
- проверьте в поисковых системах номер телефона, чтобы убедиться в том, что он действительно принадлежит названной компании.

### 6. Антивозрастные продукты

Эта афера играет на желании пожилых людей выглядеть моложе. Мошенничество с антивозрастными продуктами имеет несколько форм:

1. Как только покупатель вводит данные своей банковской карты для приобретения такого продукта, мошенники крадут деньги.

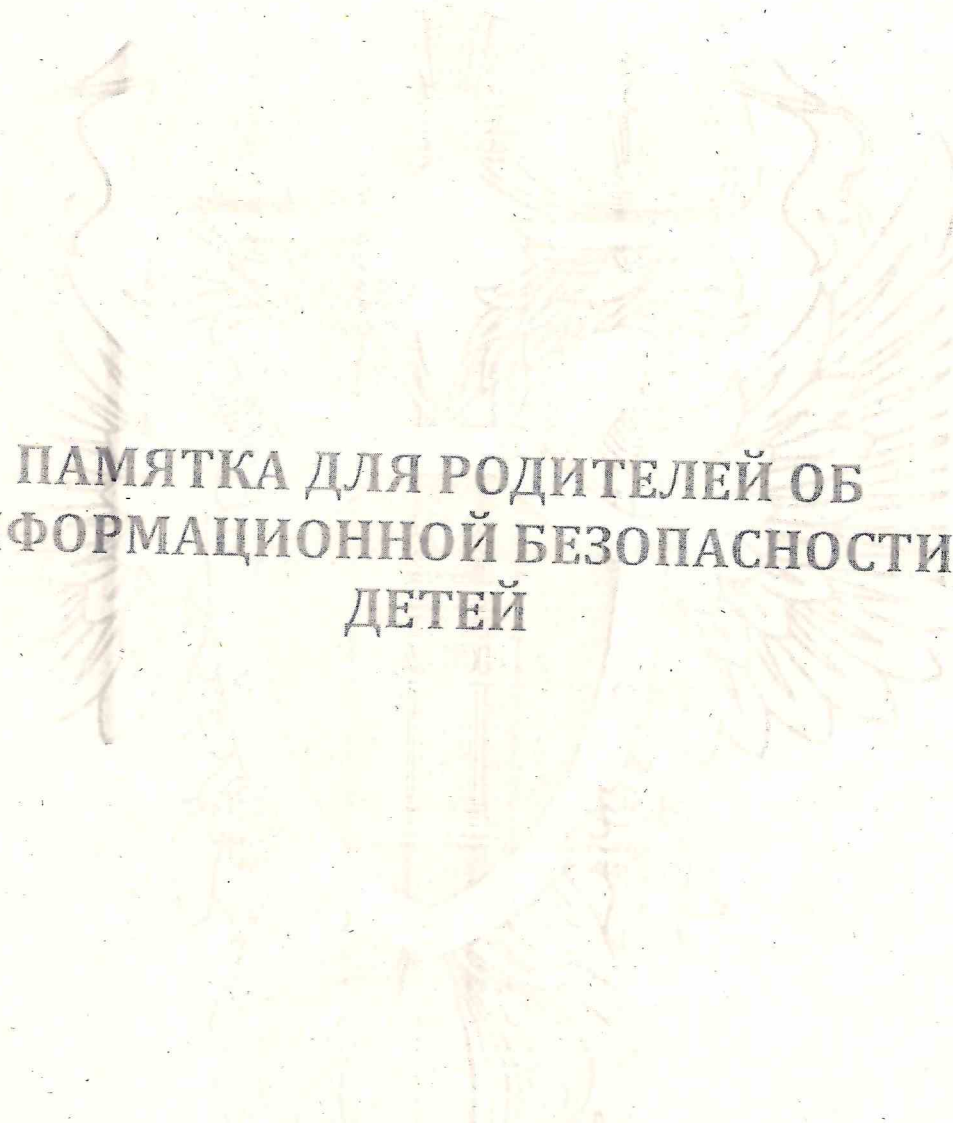
2. В другой ситуации есть вероятность столкнуться с поддельным ботоксом, который избавит от морщин. Было обнаружено, что эти поддельные продукты содержат канцерогенные компоненты, такие как мышьяк, бериллий или кадмий. Такие мошенники забирают деньги и оставляют граждан с проблемами со здоровьем.

**Как избежать афер с антивозрастными продуктами:**

- будьте осторожны с продуктами, которые имеют «секретные формулы» или «прорывные ингредиенты»;
- проверьте информацию по такому продукту, чтобы знать, какие ингредиенты он содержит и какие отзывы имеет;
- проконсультируйтесь по данному продукту с доктором.

*Берегите своих родных и близких и расскажите им о безопасности в сети «Интернет».*

Всеволожская  
городская прокуратура



**ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ ОБ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
ДЕТЕЙ**

2023

## Общие рекомендации

Дети и подростки используют интернет по-разному и для разных целей по мере взросления. Родители детей из каждой возрастной группы беспокоятся о разных вещах и хотят контролировать разные действия. Однако есть набор общих рекомендаций, которые следует помнить родителям детей и подростков любого возраста.

### Храните имена пользователей и пароли в безопасности

Для многих используемых детьми веб-сайтов требуется имя пользователя и пароль. Убедитесь, что дети знают, что эту информацию нельзя передавать никому, даже друзьям. Возможно, никто не хочет причинить ребенку никакого вреда, но даже в розыгрышах из лучших побуждений что-то может пойти не так и доставить неприятности. Храните имена пользователей и пароли в секрете и обязательно меняйте пароли, если подозреваете, что кто-то мог их узнать.

### Периодически меняйте пароли

Наряду с напоминанием детям о том, что никому нельзя сообщать свои пароли, также рекомендуется периодически менять пароли. Утечки данных происходят постоянно, а утечка паролей подвергает риску кражи личных данных и другим проблемам с кибербезопасностью. Настройте расписание смены паролей учетных записей каждые 3-6 месяцев или каждый раз, когда платформа сообщает о взломах или утечках данных. Вы можете использовать менеджер паролей, чтобы отслеживать все свои пароли в интернете и упростить их поиск вашим детям.

### Не разглашайте личную информацию в интернете

Дети и подростки не должны сообщать никому в интернете свое полное настоящее имя, адрес, район проживания, номер телефона и прочие данные. Общее правило: никогда не сообщать информацию, которая могла бы помочь интернет-хищникам найти их. Даже небольших деталей, таких как название школы или спортивной команды, достаточно, чтобы раскрыть личность. Если дети используют сайты, позволяющие общаться с незнакомцами, например, платформы социальных сетей, убедитесь, что они знают, что эта информация является конфиденциальной.

### Будьте внимательны в социальных сетях

Действия детей и подростков в социальных сетях требуют особой осторожности и внимания. Интернет огромен, но компрометирующие фотографии, грубые комментарии и личная информация могут оставить сильный след, и часто навсегда. Напомните детям, что все опубликованное в интернете сразу становится общедоступным, и любой может увидеть это. Даже частные учетные записи иногда подвергаются утечкам или атакам злоумышленников. Если вы не хотите, чтобы какой-либо неприятный момент повторялся и тревожил ваших детей, объясните им, что нужно внимательно относиться своим публикациям.

### Используйте надежное решение для кибербезопасности

Установите приложение, которое поможет защитить детей, когда они находятся в сети. Некоторые из них можно использовать на всех устройствах вашего ребенка. Оно состоит из двух приложений: одно нужно установить на устройство ребенка, второе – на смартфон родителя, чтобы просматривать отчеты и менять настройки. Встроенный родительский контроль даже позволяет управлять временем, которое дети проводят перед экраном на разных устройствах.

## Проверяйте возрастные ограничения

Многие приложения и веб-сайты имеют собственные возрастные ограничения для создания учетных записей, просмотра и регистрации. Но проблема в том, что на большинстве таких сайтов фактически нет функции проверки возраста. Например, Facebook, Snapchat и Myspace разрешают доступ только с 13 лет, но дети могут указать другой возраст и зарегистрироваться в любом случае.

## Объясните опасность передачи геоданных

Почти все современные приложения и веб-сайты имеют функции отметки геопозиции или передачи данных о местоположении. Дети и подростки должны знать, чем опасно сообщать о своем местоположении, и что не следует неосознанно соглашаться с таким условием: во всплывающих окнах приложений о местоположении подвергает детей различным опасностям: от сетевых интернет-хищников, которые могут найти их, до риска кражи личных данных. Убедитесь, что дети понимают, что означает, когда в приложении спрашивается, можно ли передавать данные о местоположении.

## Создайте список правил использования интернета

Один из лучших способов управлять использованием интернета детьми всех возрастов – это сесть и совместно составить список правил использования интернета в соответствии с их потребностями. Вы можете показать ребенку сайты для детей и подростков, поговорить о том, почему важно установить правила, и попросить их поделиться, если они чувствуют себя некомфортно или ему угрожает что-то, найденное в интернете, и т. д. Установите границы, но будьте реалистом.

## Используйте одинаковые правила при общении онлайн и лично

Научите детей тому, что к онлайн и к личному общению применимы одни и те же правила. При общении в интернете и написании комментариев лучше оставаться добрым и вежливым, не следует писать ничего такого, что не смогли бы сказать в лицо. Это также применимо и при анонимной публикации сообщений. Публикация обидных и грубых вещей – это не только некрасиво и неприятно по отношению к другим, но также может навредить репутации вашего ребенка.

## Установите родительский контроль

Настройте и пересмотрите параметры родительского контроля на всех своих устройствах в соответствии с возрастом ваших детей. Это поможет защитить детей от доступа к неприемлемому контенту в интернете. Параметры контроля можно настроить несколькими способами: например, обеспечить доступ детей только к соответствующему их возрасту контенту, установить время использования устройства, контролировать активность и запретить передачу личной информации. В дополнение к родительскому контролю можно также использовать инструменты фильтрации и мониторинга. Периодически проверяйте и обновляйте эти программы. Здесь приведена информация о потенциально опасных для детей приложениях и веб-сайтах.

## Используйте антивирусные программы

Помимо родительского контроля, используйте на всех устройствах антивирусные программы. Они защищают подключенные к интернету устройства от входящих угроз, а также выявляют, уничтожают и предупреждают о возможных угрозах для системы. Антивирусные программы не отстают от современных угроз и помогают обнаруживать новые постоянно появляющиеся вирусы.

## Расскажите о существовании фальшивых рекламных объявлений

Обсудите с детьми рекламные программы и мошенничество, связанное с фальшивыми рекламными объявлениями, с которыми они могут столкнуться в интернете. Некоторые объявления выглядят как реальные предложения, побуждающие загрузить фальшивое приложение, зарегистрироваться для участия в розыгрыше или предоставить личную информацию в обмен на бесплатные продукты. Они также могут быть представлены в виде ссылок, которыми можно поделиться с друзьями или опубликовать в социальных сетях. Если дети знают о существовании таких видов рекламы и мошенничества, они с меньшей вероятностью попадутся на них, столкнувшись в Интернете.

## Объясните детям об опасности личных встреч с незнакомцами

Дети никогда не должны лично встречаться с незнакомцами, с которыми они общались в интернете, если за такой встречей не наблюдает родитель. Объясните детям и подросткам, что не следует общаться с незнакомцами лично. Интернет-хищники или участники кибербуллинга (травли) могут скрывать, чтобы ребенок не понял, что общается с кем-то из интернета.

## Мониторинг истории поиска в интернете

Родителям детей любого возраста рекомендуется периодически проверять историю браузера, чтобы понять, какие сайты посещают их дети. Убедитесь, что в настройках браузера включено отслеживание истории, и проверяйте ее на всех устройствах с доступом в интернет. Если вы столкнетесь с подозрительными сайтами, спросите о них у ребенка. Проявите детям максимальную открытость при отслеживании их действий в интернете, чтобы они не ощущали, что за ними шпионят.

Обеспечение безопасности детей в интернете так же важно, как и в реальном мире. Существует множество причин, по которым дети хотят и должны использовать интернет: от выполнения школьных заданий до посещения виртуальных мероприятий, внеклассного обучения и интерактивных игр с друзьями. Интернет – это богатый ресурс и интересное место для общения, если дети и подростки знают, как использовать его безопасно и избегать потенциальных угроз.

Безопасность в интернете достигается постоянными разговорами с детьми о том, как и для чего используется интернет, и знанием, как обеспечить их защиту. Понимание того, почему дети выходят в интернет, с кем они там взаимодействуют и какие сайты посещают, очень важно для обеспечения их безопасности. Также крайне важно информировать их о рисках, связанных интернетом, о безопасном и вежливом общении в интернете и о действиях в случае, если они столкнулись с чем-то неуместным.



# БЕЗОПАСНЫЙ ИНТЕРНЕТ – ДЕТЯМ!

## Правила безопасного Интернета:

- никому и никогда не разглашай свои пароли. Они – твой главный секрет. Придумай свой уникальный пароль, о котором никто не сможет догадаться. Не записывай пароли на бумажках, не храни их в открытом доступе. Не отправляй свои пароли по электронной почте;
- при регистрации на сайтах и в социальных сетях старайся не указывать личную информацию (свои фамилию, имя, отчество, номер телефона, адрес места жительства, школы, место работы родителей и другое) – она может быть доступна всем, даже тем, кого ты не знаешь;
- помни, что фотография, размещенная в Интернете доступна для просмотра всем. Старайся не размещать фото, на которых изображена твоя семья, школа, дом и другие личные данные;
- не встречайся с теми, с кем ты знакомишься лишь в Интернете;
- помни, что многие люди рассказывают о себе в Интернете неправду, в том числе сведения о возрасте и половой принадлежности;
- в Интернете и социальных сетях старайся общаться только с теми, с кем ты лично знаком. Подумай и посоветуйся с родителями, прежде чем добавить незнакомого человека к себе в список «друзей»;
- не используй веб-камеру при общении с незнакомыми людьми, помни о необходимости сохранять дистанцию с незнакомцами;
- уважай собеседников в Интернете. Никогда и ни при каких обстоятельствах не угрожай другим, не размещай агрессивный и провокационный материал. Будь дружелюбен. Не груби;
- не вступай в незнакомые сообщества и не распространяй по чей-либо просьбе информационные, провокационные и агрессивно-настроенные материалы и сообщения;
- не все, что ты можешь прочесть или увидеть в интернете – правда. Не ленись и перепроверяй информацию в других поисковых системах или спроси у родителей;
- помни, что существуют сайты, непредназначенные для детей, не заходи на сайты «для тех, кто старше 18 лет», на неприличные и агрессивно настроенные сайты. Если ты попал на такой сайт по ссылке, закрой свой браузер, используя клавиши «ctrl+alt+delete»;
- расскажи все, что ты увидел, выучил или узнал нового взрослому. Доверяй своим родителям, поскольку только они смогут помочь в трудной ситуации;
- никогда не указывай свой номер телефона или электронный адрес, не отправляй с него смс-сообщения на незнакомые номера в Интернете. Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать;
- если тебе показалось, что твои друзья отправляют тебе «странную» информацию или программы, переспроси у них, отправляли ли они тебе какие-либо файлы. Иногда мошенники могут действовать от имени чужих людей, в том числе твоих друзей и родственников;
- если ты хочешь купить в Интернете какую-либо услугу или игру, обратись к взрослому. Он подскажет тебе, как избежать мошенничества;
- не загружай файлы, программы или музыку без согласия взрослых – они могут содержать вирусы и причинят вред компьютеру.

Всеволожская городская прокуратура