Лайф-хаки для безопасности в Интернет-пространстве

Не будьте излишне доверчивы:

Перед переводом средств людям, убедись в том, что вас не обманывают. Для этого необходимо запросить доказательства того, что вы общаетесь с реальным человеком, а также, иметь в случае чего, варианты возврата средств или собственной безопасности (Знать персональные данные человека, кому вы планируете переводить средства).

Не разглашайте личные данные незнакомым персонам. Это позволит вам обезопасить себя от лишней ответственности, так как если у злоумышленников будут все ваши данные, они могут представляться в интернете вами, и от вашего лица совершать преступления.

Кроме того, имея ваши персональные данные, можно легко подтвердить факт выполнения операции вами, даже, если вы эту операцию не совершали (например, оформление кредитов, микрозаймов и прочее).

Общайтесь во время купли-продажи исключительно в чате сервиса маркет-плейса. Все существующие маркет-плейсы позволяют покупателям обезопасить себя, т.к. в диалогах маркет-плейса злоумышленник не сможет запросить у вас оформить денежный перевод на себя без последствий.

При замеченных акциях, удостоверьтесь в ее истинности у официального представителя компании. Выгодные предложения всегда привлекают внимание человека и существуют случаи, когда злоумышленник предлагает вам приобрести товар с крупной скидкой, и не совсем бдительный покупатель может с легкостью заинтересоваться товаром и по итогу остаться без товара, а также, без денег.

При совершении платежей пользуйтесь функцией одобрение перевода, чтобы избежать случайных необоснованных переводов, в которых вы не уверены. «Одобрение перевода» - функция, с помощью которой ваш родственник, или доверенное лицо сможет отслеживать кому и сколько денег вы собираетесь перевести. Это будет дополнительной проверкой безопасности перевода со взглядом «со стороны».

Доступ к микрофону, геолокации и прочим данным необходим очень маленькому количеству приложений. Старайтесь как можно чаще отклонять разрешение на пользования приложениям, которые предлагают разрешение доступа к вашим данным и техническим средствам. Например, если приложение типа «Калькулятор» запросит у вас доступ к контактам, это выглядит подозрительно.

Скорее всего, вы установили вредоносную программу, от которой необходимо избавиться. Постоянно задумывайтесь о том,

для каких целей приложение запрашивает доступ к тем или иным данным.

Хранить несколько карт для различных покупок в сети, чтобы при атаке или утечке данных, у злоумышленников было нечего у вас украсть. Желательно иметь специальную карту для покупок в сети, которая постоянно будет пустой. Если вы хотите что-то приобрести, переводите на эту карту конкретную сумму средств для приобретения товара, и только после этого - совершайте покупку.

Регулярно проверять оригинальность сайта, на котором вы находитесь, чтобы не занести вредоносное программное обеспечение, которое:

- может навредить вашему устройству;
- заражает ваши файлы;
- искусственно нагружает устройство, из-за чего оно будет невыносимо медленно работать;
- может удалять те или иные файлы;
- полностью уничтожит операционную систему;
- может подгрузить другие виды вирусов.

ВАЖНО! Не открывайте приложения не впопад

Существуют сайты, которые предлагают пользователю сгенерировать пароль для своей учетной записи. Ни в коем случае, не принимайте подобные предложения. Вероятнее всего, данный сайт не просто сгенерирует вам пароль, но и запомнит его вместе с вашим логином, а это значит, что злоумышленники будут обладать вашими данными от аккаунта и смогут без труда авторизоваться за вас и в будущем, управлять вашим аккаунтом, как им вздумается.

Критерий определения того, что перед вами официальный сайт:

- удостовериться в официальности сайта можно посредством проверки адресной строки. Адресные строки в интернете уникальны, как адрес дома. Если какая-то адресная строка уже занята, мошенники не могут использовать тот же адрес. Им необходимо добавить дополнительные символы в уже существующее название официального сайта. (Например не «www.gosuslugi.ru», а «www.russians_gosUslugi124.ru»).

ВАЖНО! Адреса официальных сайтов не имеют в себе сокращений или дополнительно написанных символов или лишних слов. В случае, если присутствуют лишние слова или символы, значит сайт не официальный. Это значит, что на этом сайте ни в коем случае нельзя заполнять никаких окон, давать разрешений на обработку Cookies-файлов (файлы, который собирают различные сайты для получения информации о вашем посещении), и тем более, не нажимать никаких кнопок скачиваний. ОБРАЩАЙТЕ ВНИМАНИЕ!

Вредоносные программы могут собирать личную информацию, например:

- сохранять все что вы печатаете;
- вести круглосуточную запись микрофона или веб-камеры;
- вести запись вашего экрана;
- скачивать файлы с вашего устройства.

Чтобы не утерять данные или не перевести деньги мошенникам, которые подделывают сайты. ФИШИНГОВЫЕ САЙТЫ – специальные сайты, которые созданы злоумышленниками для добычи ваших данных:

- пароли, которые вы сохраняете для быстрого входа на ту или иную страницу;
- cookie-файлы;
- ваш IP-адрес, являющийся уникальным, который позволяет идентифицировать ваше географическое местоположение;
- формы анкет, которые вы оставляли на возможно безопасных сайтах, вводя свои ФИО, номер телефона, адрес проживания или регистрации, электронную почту и прочие данные, которые когда-то требовала анкета.
- данные кредитных карточек.

Скачивание программного обеспечения и потребление контента:

- программный продукт необходимо скачивать исключительно с официальных сайтов. Процесс нажатия на кнопку «Скачать» или «Установить» в 99% случаев приведет к занесению вируса на ваше устройство.

Любая программа, которая вам необходима имеет официальный сайт, где можно приобрести ключ к ее активации. Скачивая нелицензированный продукт, вы нарушаете закон об интеллектуальной собственности и подвергаетесь огромному риску заражения вашего устройства.

Антивирусы.

Если вы пользуетесь операционной системой Windows (7, 8, 8.1, 10, 11), то в вашу систему уже встроен хороший антивирус, который будет блокировать все вредоносные программы, которые могут содержаться на просторах интернета.

Для дополнительной защиты вы можете поставить антивирус на ваше устройство, но ни в коем случае не устанавливайте бесплатные или подозрительные антивирусные системы. Зачастую, бесплатный антивирус, скорее всего, сам окажется вирусом, который только нагрузит ваше устройство.

Антивирус может быть бесплатным, если это какая-нибудь очень урезанная или демонстрационная версия общеизвестных антивирусных систем по типу CCleaner, KasperskyLab или Avast, которые максимум смогут проверить поверхность ваших файлов и не выявят более проворных вирусов.

В случае, если же вы, все-таки, хотите поставить на свое устройство дополнительный антивирус, то лучше приобрести лицензированный продукт от проверенных компаний.

Родительский контроль.

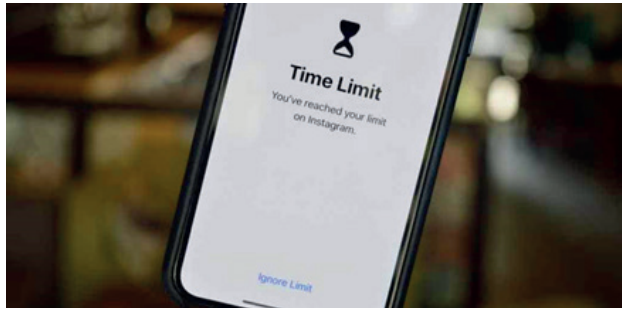
В наши дни очень много всего можно сделать с помощью телефона, например, оплатить счета, оформить покупку и потреблять огромное количество контента, который не всегда подлежит фильтрации и тем более цензуре. Поэтому, очень важно обезопасить своих детей от вредного контента, или же нежелательных трат семейных финансов.

• Обязательная установка родительского контроля на телефон своего ребенка. Это можно сделать при любых технических возможностях:

У вас и у вашего ребенка телефон с системой IOS:

В этом случае, существует функция «Экранное время», которую можно найти в главном меню настроек IPhone с версией IOS 12 и выше.

Данная функция позволяет настроить связь между устройствами родителя и ребенка. С устройства родителя, пользователь может выставлять устройству ребенка контроль на пользование приложениями по времени, ограничение на установку приложений, контроль за покупками контента, контроль денежных переводов и установку фильтров на контент из мессенджеров, браузера и видео-хостингов.



- у вас и у вашего ребенка телефон с системой Android;
- у вас IOS, а у ребенка Android;
- у вас Android, а у ребенка IOS.

В остальных трех случаях необходимо устанавливать Family Link – сервис от Google, который позволяет родителю так же вести полный контроль над пользованием ребенком телефона. Ограничение времени пользованием устройством и отдельными приложениями, ограничение на установку приложений и покупку контента в виртуальных магазинах и фильтры на контент в мессенджерах, браузере и видеохостингах. Family Link можно пользоваться так же, если у вас и у вашего ребенка система на IOS.

Пример использования родительского контроля:
Предположим, вы выставили своему ребенку 4 часа пользования устройством в сутки. Он потратил это время, и после этого его устройство блокируется, у него даже не будет возможности осуществить исходящий звонок, а если вы попытаетесь ему набрать, то вам так же ответит автоответчик, так как телефон будет считаться выключенным. В таком случае, у вас есть возможность продлить время пользования с помощью введения пароля, и дозвониться до своего ребенка. Но так как ваш ребенок дозвониться до вас со своего устройства не сможет, он должен иметь ввиду, что при чрезмерном пользовании устройством, он может потерять доступ ко всем функциям своего устройства.

Важно знать - во что играет ваш ребенок. Для этого можно отслеживать загрузки приложений с помощью родительского контроля.

Если к аккаунту вашего ребенка привязана ваша банковская карта:

С развитием интернета и коммуникационных технологий мошенникам стало очень просто обманывать юных и наивных игроков отправлять им деньги родителей. Всегда фиксируйте и регулярно проверяйте на что вы тратили деньги в приложениях ваших банков (Сбербанк, ВТБ, Тинькофф, Альфа-банк и др.) в разделе «История», где описывается история ваших транзакций и покупок.

В случае, если вы заметили подозрительную транзакцию или покупку, немедленно выясните куда ушли деньги, и кто мог осуществить данную операцию. В случае, если ваш ребенок в тайне от вас оплатил что-то в игре, или отправил кому-то деньги, желательно незамедлительно перевести все средства с это карты на другую и заблокировать этот счет в банке, чтобы потенциальный злоумышленник не смог загнать ваш счет в долги.

Контроль за покупками при помощи приложений родительского контроля, даст возможность знать о намерениях осуществить приобретение самой игры или покупку внутри игры.

Многие игры предлагают тратить реальные деньги, зачастую большие суммы, на покупку предметов, которые, например, украшают объекты в игре или же специальные предметы, купив которые, будет легче побеждать и многое другое.

Своевременный контроль даст родителю возможность повысить финансовую грамотность ребенка и провести дополнительные воспитательные меры.