Содержание:

Информационная безопасность в среде Интернет

Огромную часть нашей жизни мы проводим в интернете онлайн, сидя за нашим компьютером и телефоном, который не выпускает из рук днями. Всё чаще и чаще мы проводим своё время в интернет сети, но и при этом забываем про свою бдительность, чем пользуются наши сетевые враги - мошенники. Какие ошибки допускают 95% пользователей интернетом? Правила информационной безопасности в интернет сети, которые должен запомнить и знать каждый из нас.

Мы чаще стали уходить из реальной жизни в виртуальную, но люди и представь себе не могут какая опасность скрывается в стенах виртуальной жизни, идущая от информационной среды. Мы очень беспечны и наивны, что приводит к последствиям отрицательного характера.

Вспомним даже как же часто обманывают дедушек и бабушек различные мошенники, которые ходят по домам и квартирам. Сейчас появилось много современных мошенников и жуликов, которые охотятся на людей в интернете, они придумают различные способы обмана с каждым днём, чтобы в сети аферистов попали как можно больше людей.

Наш современный мир сделал мошенников более хитрыми, изощренными и коварными. В ход идут различные и многочисленные способы схем мошенничества, которые с трудом можно ожидать и предусмотреть. Но есть решение: Нужно стать более подкованными в информационной безопасности и знать схемы мошенников, чтобы не попасть в их сети. Для этого надо иметь информационную грамотность, то есть знать правила в информационной сети.

Какая опасность поджидает нас в интернете

Какая же всё-таки исходит опасность в цифровом пространстве? Вы скажите: это же лишь всего-навсего интернет! Но я скажу, что существует море опасностей,

которые могут причинить колоссальный вред обыкновенному пользователю, который по своей неграмотности попадет в ловушку мошенников. Какие последствия могут быть?

1. Приватность и анонимность, когда может пострадать ваша репутация, карьера и жизнь

Это очень важный пункт, так как уже много человек попалось на эту удочку и теперь страдают. Вы можете подвергнуться разным видам шантажа от мошенника. Например, существует какая-то информация или фотографии, которые могут подорвать репутацию в реальной жизни, они могут находиться в личных архивах, но если мошенник сможет до них добраться, у него появляются рычаги давления на вас. Он может применить шантаж, потребовать высокую сумму чтобы не распространять эту информацию в массы и ваше окружение, например, не скинуть коллегам по работе или вашему начальнику. Отчаянные люди платят огромные суммы таким людям, а некоторые отказываются и теряют работу, семью и им даже приходится переезжать в другое место.

2. Финансовые онлайн-транзакции и снятие денег с ваших счетов

Очень часто людям звонят мошенники, представляются они сотрудниками банка и говорят, что с вашей карты пытаются сделать перевод на большую сумму денег и подтверждаете ли Вы этот перевод. Когда вы отказываетесь, то якобы «сотрудники банка» пытаются заблокировать счет и спрашивают конфиденциальную информацию, ваши персональные данные, а именно номер карты, логин и пароль к доступу вашему аккаунту в онлайн банке. И если вы передадите эти данные мошеннику, то они сделают перевод на свою карту с вашего счета.

3. Кибербуллинг и преследование другими людьми

В социальных сетях очень распространен сталкеринг, это когда какой-то человек пристально следит за жизнью другого человека. Но бывает такое что эта пристальная слежка выходит из онлайн в офлайн и с помощью социальных сетей, человек начинает следить уже в реальной жизни, благодаря из информации, которую вы выкладываете в «истории» или фотографии, о своем местоположении.

Так же кибербуллинг – это издевательство, насмешки со стороны других пользователей по отношению к Вам. Одна из серьезных проблем современности, потому что очень часто, если кибербуллингу подвергается неокрепшая психика (например, детская), то человек может от неё пострадать, например, совершить попытку суицида или наоборот совершить какое-либо преступление.

4. Потеря аккаунтов в социальных сетях, управление группами и сайтами

Когда вы можете потерять доступ к своим социальным сетям и аккаунтом, доступ оказывается в руках посторонних людей и этот человек может использовать этот доступ в плохих целях, например, диалоги с какими-то людьми, пересылать другим людям (фото или видео вашему начальнику/жене/мужу и т.д).

5. Кража конфиденциальной информации: фотографии, паспортные данные, номер банковской карты

Благодаря паспортным данным, на владельца паспорта можно навесить множество кредитов и долгов, через такие сервисы как «Быстрые деньги». Так же опасно загружать в сеть фотографию своего лица с паспортом рядом, так как часто такую фотографию просят на процедуре подтверждения личности, чем злоумышленники активно пользуются.

6. Рассылка СПАМа со своих аккаунтов или почты

7. Причинение вреда ближнему окружению, которое введено в заблуждение киберпреступниками.

Например, есть распространенная практика, когда с незнакомого номера телефона приходит СМС вашем близким или родителям о том, что это Вы и вы попали в аварию, поэтому просите переслать определенную сумму денег на карту. На почве страха близкие могут переслать деньги.

Правила информационной безопасности в интернете

1. Держите личную информацию профессионально и ограниченно

Потенциальным работодателям или клиентам не нужно знать ваш личный статус или домашний адрес. Им нужно знать о вашем опыте и профессиональном опыте, а также о том, как с вами связаться. Вы не стали бы раздавать чисто личную информацию незнакомцам индивидуально - не передавайте ее миллионам людей в Интернете.

2. Не отключайте настройки конфиденциальности

Маркетологи любят знать о вас все, и хакеры тоже. Оба могут многому научиться из вашего просмотра и использования социальных сетей. Но вы можете взять на себя ответственность за свою информацию. В веб-браузерах, и в мобильных операционных системах есть настройки для защиты вашей конфиденциальности в Интернете. На крупных веб-сайтах, таких как Facebook, также доступны настройки повышения конфиденциальности. Эти настройки иногда (намеренно) трудно найти, потому что компании хотят, чтобы ваша личная информация имела маркетинговую ценность. Убедитесь, что вы включили эти меры защиты конфиденциальности и оставьте их включенными.

3. Практикуйте безопасный просмотр

Вы бы не выбрали прогулку по опасному району - не посещайте опасные районы в Интернете. Киберпреступники используют зловещий контент в качестве приманки. Они знают, что людей иногда соблазняет сомнительный контент, и они могут ослабить бдительность, когда ищут его. Интернет-полусвет полон труднодоступных ловушек, где один неосторожный щелчок может раскрыть личные данные или заразить ваше устройство вредоносным ПО. Сопротивляясь побуждению, вы даже не даете хакерам шанса.

4. Убедитесь, что ваше интернет-соединение безопасно.

Когда вы выходите в Интернет в общественном месте, например, используя общедоступное соединение Wi-Fi, то у вас нет прямого контроля над его безопасностью. Эксперты по корпоративной кибербезопасности беспокоятся о «конечных точках» - местах, где частная сеть соединяется с внешним миром. Ваша уязвимая конечная точка - это ваше локальное Интернет-соединение. Убедитесь, что ваше устройство безопасно, и, если сомневаетесь, дождитесь лучшего времени (т.е. Пока вы не сможете подключиться к защищенной сети Wi-Fi), прежде чем предоставлять такую информацию, как номер вашего банковского счета.

5. Будьте внимательны при загрузке

Главная цель киберпреступников - заставить вас загрузить вредоносное ПО - программы или приложения, которые несут вредоносное ПО или пытаются украсть информацию. Это вредоносное ПО может быть замаскировано под приложение: от популярной игры до того, что проверяет трафик или погоду. Не загружайте приложения, которые выглядят подозрительно или поступают с сайта, которому вы не доверяете.

6. Выберите надежные пароли.

Пароли - одно из самых слабых мест во всей структуре Интернет-безопасности, но в настоящее время их нет. Проблема с паролями заключается в том, что люди обычно выбирают простые для запоминания (например, «пароль» и «123456»), которые кибер-ворам также легко угадать. Выбирайте надежные пароли, которые киберпреступникам труднее разоблачить. Программное обеспечение менеджера паролей может помочь вам управлять несколькими паролями, чтобы вы их не забыли. Надежный пароль - это уникальный и сложный пароль длиной не менее 15 символов, состоящий из букв, цифр и специальных символов.

7. Совершайте покупки в Интернете с безопасных сайтов.

Каждый раз, когда вы совершаете покупку в Интернете, вам необходимо предоставить информацию о кредитной карте или банковском счете - именно то, что киберпреступники больше всего хотят заполучить. Предоставляйте эту информацию только тем сайтам, которые обеспечивают безопасные зашифрованные соединения. Вы можете идентифицировать защищенные сайты, ища адрес, который начинается с https: (S означает безопасный), а не просто http: Они также могут быть отмечены значком замка рядом с адресной строкой.

8. Будьте осторожны с тем, что публикуете

Любой комментарий или изображение, которое вы публикуете в сети, могут оставаться в сети навсегда, поскольку удаление оригинала (например, из Twitter) не приводит к удалению копий, сделанных другими людьми. У вас нет возможности «забрать назад» замечание, которое вы бы не сделали, или избавиться от смущающего селфи, сделанного на вечеринке. Не размещайте в Интернете ничего, что вы бы не хотели, чтобы увидела ваша мама или потенциальный работодатель.

9. Будьте осторожны с тем, кого вы встречаетесь в Интернете

Люди, которых вы встречаете в Интернете, не всегда те, за кого себя выдают. Более того, они могут даже быть ненастоящими. Фальшивые профили в социальных сетях - это популярный способ хакеров, чтобы подружиться с неосторожными пользователями Интернета и обчистить их кибер-карманы. Будьте осторожны и разумны в своей социальной жизни в Интернете, как и в личной общественной жизни.

10. Своевременно обновляйте антивирусную программу.

Программное обеспечение для обеспечения безопасности в Интернете не может защитить от всех угроз, но оно обнаружит и удалит большинство вредоносных программ, хотя вы должны убедиться, что оно актуально. Будьте в курсе обновлений вашей операционной системы и приложений, которые вы используете. Они обеспечивают жизненно важный уровень безопасности.