Доклад на тему «Основы безопасного поведения в сети Интернет»

Всем известно, что современные компьютерные технологии стремительно развиваются и занимают всё больше места в жизни человека. Уже в 2022 году использование Интернета среди населения России составило 79% или более 116 млн. человек (по данным Фонда общественного мнения), и данный процесс продолжает стремительно развиваться.

Стремительно изменяется культура труда и возрастает роль фундаментального образования, обеспечивающего профессиональную мобильность человека, его готовность к освоению новых технологий, в числе информационных.

Мы используем компьютерные технологии с целью облегчения рутинных педагогических действий для осуществления качественного, индивидуального, дистанционного обучения.

Производим поиск, хранение и передачу необходимой нам информации в цифровом виде и в интернет-пространстве, публикуем различные статьи с соблюдением авторского права при использовании информационных продуктов, улучшаем навыки общения с другими пользователями, формируя таким образом информационную и коммуникативную компетентность.

Однако необходимо понимать, что, пользуясь всемирной паутиной, всегда присутствует возможность утечки Вашей конфиденциальной информации, если вы не будете соблюдать основные правила, о которых сегодня пойдет речь.

Вначале немного поговорим об основных опасностях, которые могут поджидать вас при использовании интернета.

Ниже приведен их основной список:

1. Кража персональных данных;

Данный пункт подразумевает использование чужой личной информации без согласия, для получения финансовой выгоды. Примерами личной информации являются: паспортные данные, медицинские карты, номер социального страхования, номера кредитных карт, водительского удостоверения, информация о банковском счете и связанный с ним PIN-код и другое.

2. Нанесение вреда вашему устройству посредством вредоносных программ и вирусов;
3. Фишинговые электронные письма;

Отметим, что фишинг – это совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты и другую конфиденциальную информацию.

Чаще всего злоумышленники выдают себя за представителей известных организаций в электронных письмах или телефонных звонках.

4. Поддельные (то есть фишинговые) сайты;

Это мошеннические веб-ресурсы, выманивающие реквизиты карты под видом предоставления несуществующих услуг. Такие сайты создаются как подделки популярных веб-ресурсов, которым пользователи доверяют.

Практически всегда дизайн фишинговых сайтов напоминает или даже бывает идентичен дизайну популярного сайта.

5. Неприемлемый контент;

Это не только информационные материалы (изображения, видео, аудио, тексты), содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр и т.п., но и различные вредоносные программы, задача которых — получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством.

6. Кибербулинг;

Это запугивание и травля с использованием цифровых технологий. Он может проходить в социальных сетях, в приложениях для обмена сообщениями, на игровых платформах и мобильных телефонах. Это повторяющиеся эпизоды, цель которых - напугать, разозлить или опозорить тех, кого преследуют.

Примерами онлайн-травли могут являться:

- Бойкот — игнорирование жертвы в соцсетях или обрывание связи с ней;
- Домогательство — когда агрессор регулярно угрожает жертве в интернете, задаёт неприятные, личные вопросы или шантажирует;
- Троллинг — высмеивание при помощи оскорблений;
- Аутинг — публикация личной информации без разрешения её владельца;
- Диссинг — также публикация личной информации, но той, которая может навредить репутации жертвы или разрушить её.

7. Психологические манипуляции.

Помните, что цель мошенников – с помощью психологических манипуляций побудить человека перевести деньги на их счет или совершить другие выгодные им действия.

Последнее время мошенники делают ставку не на технические средства взлома, а на знание психологии. Это называется социальной инженерией. Задача мошенника — вызвать у жертвы сильные эмоции, чтобы ею было проще управлять.

8. Мошенничество в сети Интернет;

Примерами мошенничества могут оказаться:

- Перевод денег за границу;

Аферисты говорят, что все международные переводы запрещены и уверяют: «Именно мы сможем по своим каналам переслать деньги вашим родственникам или оплатить товары и услуги за рубежом».

- Распродажа остатков уходящих брендов;

Как только иностранные компании начали приостанавливать продажи, возникли сайты с предложениями о продаже остатков нераспроданной одежды, гаджетов, бытовой техники.

Как вы успели догадаться, часто данные сайты являются фишинговыми – с их помощью аферисты выманивают данные пользователей и крадут их деньги.

— Установка нового «подозрительного» VPN;

Мошенники используют в своих интересах популярность VPN-сервисов, позволяющих обойти блокировки. Зачастую люди не вдаются в подробности, что за программу они устанавливают. Этим и пользуются аферисты. Через недобросовестный VPN они могут получить вашу личную информацию.

Никогда не устанавливайте подозрительные программы и никогда не вводите через VPN реквизиты карты и данные онлайн-банка.

— Предоставление высокооплачиваемой работы;

Мошенники могут поджидать даже на сайтах по поиску работы. Они предлагают вакансии от имени известных компаний и гарантируют высокий заработок. А по факту выманивают у людей данные и иногда вынуждают оплатить обучение, после чего отказывают в трудоустройстве, либо затягивают новичков в свою финансовую пирамиду для привлечения очередных жертв.

— Sim-карты;

Активизируются атаки, связанные с sim-картами. Схема работает так: злоумышленник в салоне сотовой связи по поддельным документам или вступив в сговор с сотрудником покупает дубликат sim-карты, которую якобы потерял, вставляет ее в свой телефон и через СМС-команды выводит деньги со счета жертвы.

Чтобы избежать перечисленных опасностей, важно знать и соблюдать основные правила работы в интернете.

1. Убедитесь, что ваше интернет – соединение защищено;

При использовании общедоступного Wi-Fi для выхода в сеть в общественном месте (кафе, отелях, аэропортах, торговых центрах и других местах) у вас отсутствует контроль над его безопасностью. Использование общедоступного Wi-Fi не всегда безопасно, однако может оказаться неизбежным, если вы находитесь вне дома. Если вы используете его используете, избегайте выполнения таких операций как онлайн-банкинг и онлайн-покупки.

Если эти операции необходимы, используйте виртуальную частную сеть (VPN), так как он обеспечивает безопасность данных, передаваемых по незащищенной сети. Если вы не используете VPN, воздержитесь от совершения личных транзакций до момента, когда появится возможность надежного подключения к интернету.

Данный совет связан с тем, что общественные Wi-Fi сети легко взломать. После чего злоумышленники получают всю информацию от подключенных устройств напрямую. Чаще всего крадут платежную информацию, сохраненные логины и пароли.

2. Используйте надежные пароли;

Пароли – одно из самых слабых мест в системе кибербезопасности. Пользователи часто создают пароли, которые легко запомнить а, следовательно, злоумышленникам не составит труда их подобрать. Кроме того, опасно использовать один и тот же пароль для нескольких сайтов, поскольку, получив учетные данные с одного сайта, злоумышленники могут получить доступ к другим сайтам, на которых используются эти же учетные данные.
Выбирайте надежный пароль, который будет обладать следующими свойствами: его длина минимум 12 символов; содержит заглавные и строчные буквы, также специальные символы и цифры; не очевидные (не использовать комбинации последовательности цифр, даты рождения и других личных вещей, легко угадываемых).

3. По возможности включите многофакторную аутентификацию;

Это способ проверки подлинности, при котором для доступа к учетной записи используются два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля, при многофакторной аутентификации запрашивается дополнительная информация:

- Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или электронную почту;
- Ответы на личные вопросы безопасности;
- Отпечаток пальца или другая биометрическая информация, например, голосовые данные или распознавание лица.

4. Убедитесь, что веб-сайты выглядят и работают надежно;

При посещении сайта обращайте внимание, имеется ли у сайта актуальный сертификат безопасности (SSL).
Это технология для формирования защищенного доступа через браузер пользователя.
Сайт, получивший такой сертификат, дает знать браузеру, что веб-страница надежна и с ней можно обмениваться данными.
Самый простой способ определить, является ли сайт безопасным, это обратить внимание на то, что веб-адрес сайта начинается с HTTPS, а не с HTTP (S означает «безопасный»), и что в адресной строке отображается значок замка.
Также для того, что определить, является ли сайт фишинговым, необходимо проверить домен (то есть название сайта) в адресной строке и сравнить его с изначальным адресом домена.
Фишинговые сайты очень часто используют похожие домены для обмана пользователей.

5. Следите, по каким ссылкам вы переходите;

Один неосторожный переход по ссылке – и ваши личные данные попадут к злоумышленникам или устройство заразится вредоносной программой. Поэтому важно внимательно переходить по ссылкам и избегать определенных типов контента: ссылок из ненадежных источников, спам-сообщений, онлайн-викторин, «бесплатных» предложений и нежелательной рекламы.
При получении электронного письма, в подлинности которого вы сомневаетесь, не переходите по содержащимся в нем ссылкам и не открывайте вложения.

6. Удаляйте неиспользуемые учетные записи;

Известно, что у многих есть устаревшие неиспользуемые учетные записи. Их наличие может стать источником уязвимостей при использовании интернета. Старые учетные записи с большей вероятностью имеют более слабые пароли, а сайты, на которых они использовались, могут иметь ненадежную политику защиты данных. Кроме того, по данным в старых профилях социальных сетей киберпреступники могут собрать о вас различные данные, например, дату рождения и местонахождение, и составить базовое представление.

7. Будьте осторожны с загружаемыми из интернета объектами;

Помните, что вредоносные программы могут быть замаскированы под различные приложения, от популярных игр до приложений для проверки трафика или погоды.
Вредоносные программы наносят ущерб: нарушают работу устройства, крадут личные данные, предоставляют несанкционированный доступ к компьютеру.
Обычно для их загрузки требуется ряд действий со стороны пользователя, но встречается также заражение путем скрытой загрузки, когда веб-сайт пытается установить вредоносные программы на компьютер, не спрашивая предварительного разрешения. Будьте осторожны при загрузке объектов на устройство, загружайте контент только из надежных или официальных источников.

8. И помните: файлы «Cookie» - не зло.

Веб-сайты отслеживают вашу активность в браузере с помощью файлов «Cookie», чтобы сделать ваш просмотр более быстрым и удобным, так как в них хранится основная информация о посещаемых вами сайтах и о том, что вы нажимаете на них.
Файлы Cookie не представляют никакого серьезного риска для вашей

онлайн – безопасности. Они просто хранят данные о входе на определенные сайты. Но в случае чего вы всегда сможете ограничить их работу или полностью отключить при необходимости.

Мною были приведены основные моменты для безопасного поведения в сети Интернет. Надеюсь, перечисленные выше советы будут вам полезны и помогут избежать утечки информации и предотвратить заражения вредоносными программами.