МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №29»

Утверждена
23.09.2024г методическим советом МБОУ СОШ №29

Методическая разработка урока по предмету «Информатика»

Разработала:
Трубарова Ия Анатольевна, учитель информатики МБОУ СОШ №29

Мытищи

Содержание

1 Общие сведения

Тема урока «Информационная безопасность (сеть Интернет)»
Класс: 9

Предмет: Информатика

Тема занятия: Безопасность в Интернете

Цели занятия:

- Сформировать понятийный аппарат обучающихся по информационной безопасности.
- Выработать ответственное отношение к информационной безопасности.
- Развить умения осуществлять поиск, анализ и интерпретацию информации.
- Развить практические навыки защиты персональной информации
- Обеспечить обучающимся возможность планировать и реализовывать собственное личностное развитие.
- Привить навыки работать в коллективе, осуществлять эффективное взаимодействие

Тип занятия: урок актуализации и открытия нового знания

Оборудование: компьютеры, электронные образовательные ресурсы, доска, проектор

2. Тайминг

№ п\п	*Этап занятия*	*Время продолжительности этапа, мин*
1	Организационное начало (этап мотивации к учебной деятельности)	3
2	Актуализация и фиксирование индивидуального затруднения в пробном действии; объяснение нового материала	15
3	Этап самостоятельной работы с проверкой	18
4	Этап включения в систему знаний и повторения	5
5	Этап рефлексии учебной деятельности на уроке. Подведение итогов.	4
		45

3. Технологическая карта

Этап занятия	Дидактические задачи этапа занятия	Виды работы, формы, методы, приемы	Содержание педагогического взаимодействия		Планируемые результаты
			Деятельность преподавателя	Деятельность обучающихся	
I. Организационное начало (этап мотивации к учебной деятельности)	Подготовка обучающихся к работе на занятии: мотивирование обучающихся к учебной деятельности посредством создания эмоционально-положительной обстановки в классе.	1. Беседа 2. Приём "отсроченная отгадка"	Приветствует обучающихся, визуально оценивает готовность к занятию. Показывает видеоролик. Просит обучающихся выдвинуть предположения о теме занятия, организуя управляемое обсуждение темы урока Организует диалог с обучающимися: Какие вопросы мы должны решить? Какие цели мы выполним?	Слушают речь учителя. Выдвигают предположения о теме занятия. В ходе обсуждения обучающиеся приходят к мысли, что на занятии будут рассматриваться вопросы безопасности в сети Интернет Осмысливают полученную информацию, настраиваются на работу.	Обучающиеся готовы к выполнению учебных задач, имеют соответствующую мотивацию

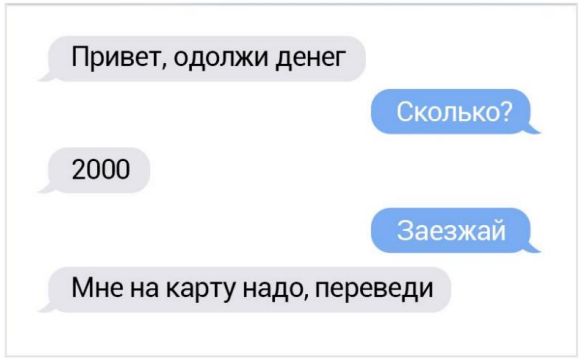
II. Актуализация и фиксирование индивидуального затруднения в пробном действии, объяснение нового материала	Формирование у обучающегося внутреннего осознания потребности открытия новых знаний и умений.	Приём «Лови ошибку!»	Демонстрирует презентацию, объясняет основные понятия, предупредив обучающихся, что в презентации допущены смысловые ошибки В случае обнаружения обучающимися ошибки, акцентирует их внимание на правильном варианте. Если обучающиеся затрудняются найти ошибки, демонстрирует их .	Смотрят презентацию. Выдвигают гипотезы. Стараются найти ошибки. Вносят коррективы, оглашают правильный вариант.	У обучающихся активизированы мыслительные процессы, необходимые для усвоения нового знания: анализ, сравнение, аналогия, классификация, синтез, обобщение.

III. Этап самостоятельной работы с проверкой	Формирование умения применять новые знания в решении учебной задачи	Прием «Поиск решения» Задание для самостоятельной работы «Решение ситуационных задач»	Предлагает решить задание для самостоятельной работы Предлагает провести взаимопроверку выполненных заданий Фиксирует результаты взаимной проверки обучающимися выполненных заданий	Самостоятельно выполняют задания. Осуществляют в взаимопроверку выполненных заданий	Обучающиеся способны к воспроизведению действий по формулированию логически последовательного, осознанного решения задачи. Обучающиеся осуществляют взаимоконтроль

VI. Этап включения в систему знаний и повторения	Фиксация полученных знаний	Прием «Верю-не верю»	Предлагает ответить в тетради на вопросы, каждый из которых начинается со слов «Верите ли Вы, что…»	Отвечают на вопросы, учитывая, что ответ на вопрос может быть только «да» (+) или «нет» (-)	Обучающиеся способны обобщать знания и формулировать выводы, полученные в ходе различных мыслительных операций и способов действий с изучаемыми объектами
V. Этап рефлексии учебной деятельности на уроке. Подведение итогов	Соотнесение обучающимися поставленных целей занятия с результатами своей деятельности.	Беседа	Просит ответить обучающихся на следующие вопросы: - Назовите тему нашего сегодняшнего занятия. - Какие цели занятия мы с вами ставили?: - Какие затруднения перед вами стояли? - Смогли ли мы преодолеть эти затруднения? Выставляет оценки за занятие	Отвечают на вопросы преподавателя.	Обучающиеся умеют формулировать выводы о достижении поставленных целей деятельности.

4. Задание для самостоятельной работы «Решение ситуационных задач»

Ведите ваши ФИО	

№	Ситуационная задача	Решение
1	На доске объявлений размещено сообщение, в котором говорится о том, что каждому обучающемуся школы для работы в Школьном портале выделяется персональный пароль. Для того чтобы обучающиеся его не забыли, пароль представляет дату рождения и имя каждого ученика. 1. Какие правила обеспечения информационной безопасности нарушены? 2. Какие символы должны быть использованы при записи пароля?	
2	Вы получили сообщение в чате соцсети от друга  Опишите ваши действия	
3	Вас объявили победителем Поздравляем! Вы стали победителем конкурса Лучшее фото дня! Вы выиграли оценивание фото на "+10." Для получения приза подтвердите свое согласие отправив СМС с текстом 70+28658 31 на номер 5777. Не упустите свой шанс! СМС сообщение бесплатно. Ваши действия	

4	Ваша подруга опубликовала запись в социальной сети Как вы оцените эту запись с точки зрения информационной безопасности? Какие последствия могут возникнуть?  	

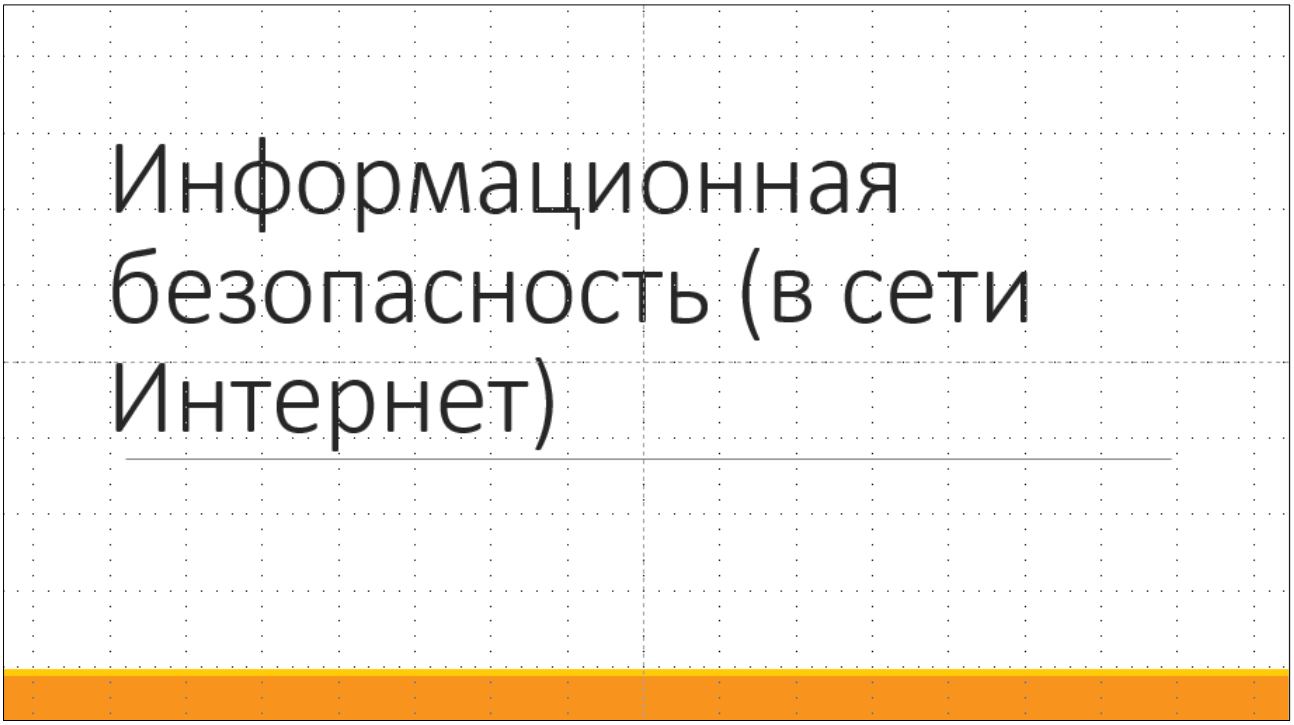
5. Оценочная карта к самостоятельной работе

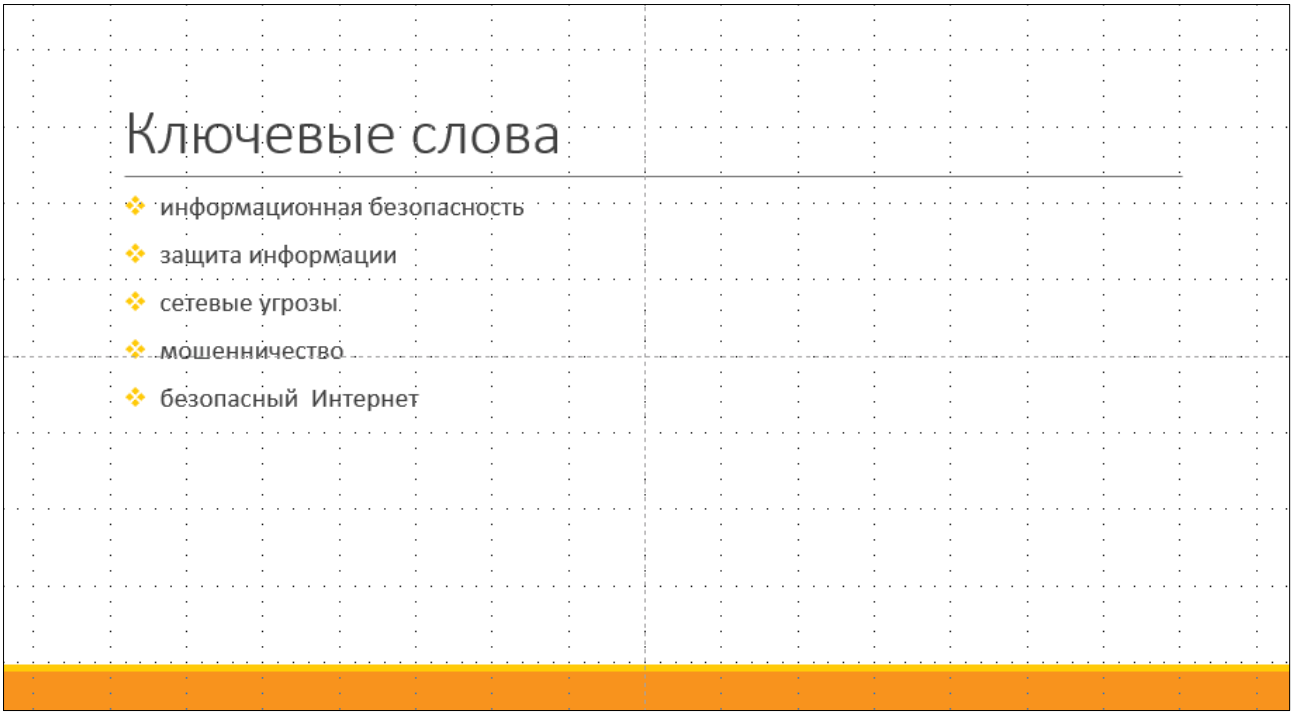
ФИО проверяемого	11-12 баллов – оценка 5 8-10 баллов – оценка 4 5-7 баллов – оценка 3 Менее 5 – оценка 2	ОЦЕНКА	

№	Ответы на ситуационную задачу	Балл
1	Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем. В качестве пароля должна выбираться последовательность символов, обеспечивающая малую вероятность её угадывания. Пароль должен легко запоминаться. Длинный: минимум 12 символов, в идеале, даже больше. Содержит заглавные и строчные буквы, а также специальные символы и цифры. Не очевидный: в пароле не используются личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного. Избегайте простых	

	последовательностей («12345», «qwerty») – такие пароли подбираются за считаные секунды. По той же причине избегайте распространенных слов («password1»). Не содержит запоминающихся сочетаний клавиш.	
2	Завладев данными для входа в аккаунт пользователя, мошенники рассылают списку его друзей слёзные сообщения с просьбами о помощи. Люди, от имени которых поступают подобные просьбы, теряют доступ к аккаунту и не могут опровергнуть написанное Нельзя сразу переводить деньги на карту. Необходимо перезвонить другу и уточнить, действительно ли он просит деньги	
3	Мошенники, рассылая по социальным сетям и почтовым адресам поздравительные сообщения с текстом о том, что пользователь выиграл приз, победил в конкурсе. Невозможно победить в конкурсе. В котором ты не учувствовал. Нельзя отправлять ответное sms, так как будут списаны деньги	
4	Подруга поступила неправильно. Не публикуйте фотографии посадочных талонов. Авиасообщение начинает возобновляться, и многие радостно публикуют на своих открытых страницах посадочные талоны на рейсы. Зачастую - со штрих-кодами, номерами рейсов и фамилиями. Чем это опасно? Тем, что любой человек, увидевший такое фото, может при желании войти в личный кабинет и как минимум отменить билеты. Информация на билетах говорит о вашем отсутствии, чем могут воспользоваться грабители	

6. ПРИМЕР презентационного материала (красным цветом обозначены интерактивные элементы)





Сеть Интернет

это **глобальная** **система взаимосвязанных компьютерных сетей**, использующая набор интернет-протоколов (TCP/IP) для связи между сетями и устройствами.

Интернет - сеть сетей, состоящая из частных, государственных, академических, деловых и правительственных сетей локального и глобального масштаба, связанных широким спектром электронных, беспроводных и оптических сетевых технологий.

Информационная безопасность

это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации

Интернет-безопасность

это безопасность действий и транзакций, совершаемых в интернете. Интернет-безопасность входит в более широкие понятия, такие как кибербезопасность и компьютерная безопасность, и включает безопасность браузера и сети, а также правильное поведение в сети.

Угрозы интернет-безопасности

- Взлом;
- Вирусы и вредоносные программы;
- Кража личных данных;
- Контентные риски;
- Коммуникационные риски;
- ~~Дистанционное обучение~~

Методы, которые помогают хакерам проникнуть в ваш аккаунт

- Перебор по словарю
- Данные из социальных сетей и другая раскрытая вами личная информация
- Брутфорс-атаки
- Фишинг
- Утечки данных

Меры компьютерной безопасности

- Активизация брандмауэра;
- Установка и обновление антивирусных программ;
- Обновление программного обеспечения.
- НЕ Открывать файлы, полученные от неизвестных корреспондентов.
- Осваивать способы борьбы со спамом и сетевым мошенничеством.
- Принимать необходимые меры предосторожности, пользуясь беспроводной связью.
- Устанавливать пароли, используя правила, использовать многофакторную аутентификацию везде, где возможно.

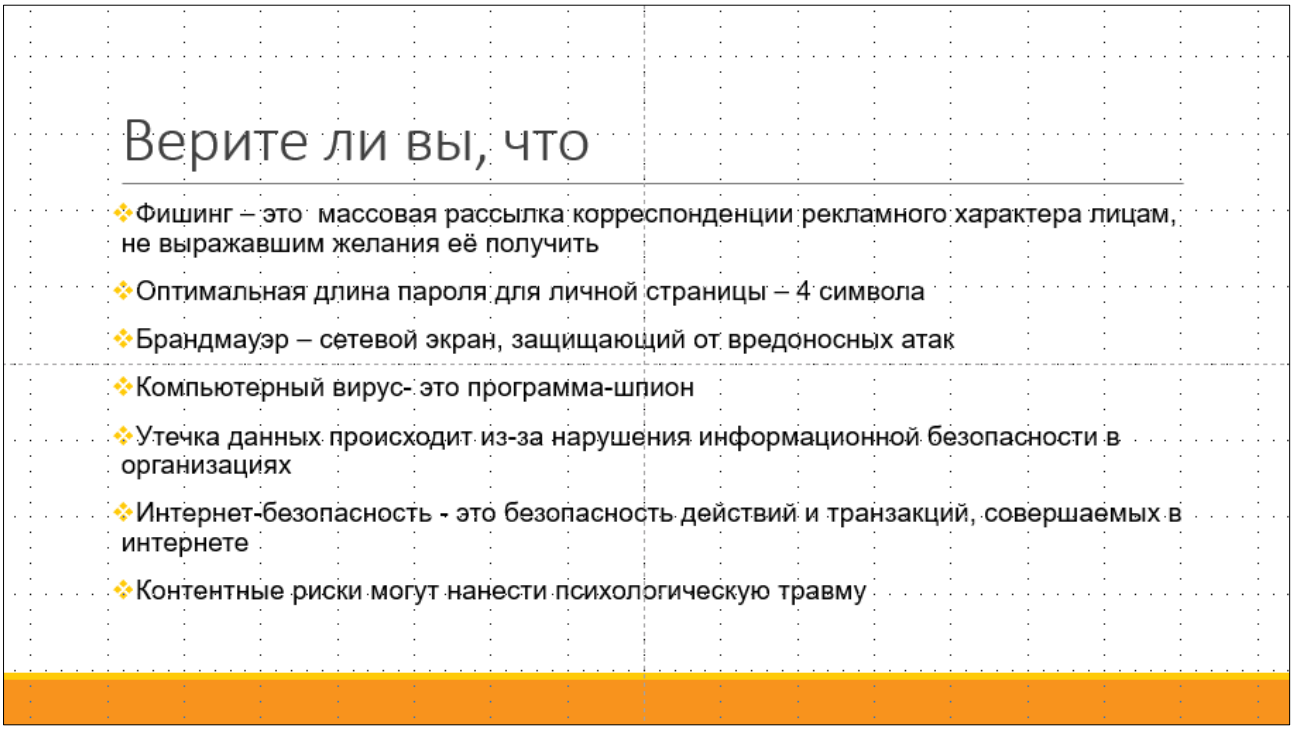
Решение ситуационных задач

1.Путь к заданию:

Рабочий стол – Общая папка – класс - Информационная безопасность

2. Открываем Файл «Решение ситуационных задач» - заполняем таблицу (предварительно файл «Сохранить как» Фамилия_ безопасность)

3. Для поиска решения используем файл «Как защитить личные данные в сети»



7. Материалы для самостоятельного изучения

КАК ЗАЩИТИТЬ ЛИЧНЫЕ ДАННЫЕ В СЕТИ

.

1. **Используйте многофакторную аутентификацию везде, где возможно**

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используется 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 адрес электронной почты.
- Ответы на личные вопросы безопасности.
- Отпечаток пальца или другая биометрическая информация, например голосовые данные или лицо.

Многофакторная аутентификация снижает вероятность кибератаки. Чтобы защитить онлайн-аккаунты, рекомендуется по возможности использовать многофакторную аутентификацию. Для обеспечения безопасности в интернете можно также можете применять сторонние приложения проверки подлинности, такие как Google Authenticator и Authy.

2. Используйте сетевой экран

Сетевой экран (брандмауэр) исполняет роль барьера между вашим компьютером и сетью, например интернетом. Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами. Часто сетевой экран входит в состав операционной системы или системы безопасности. Для обеспечения максимальной безопасности в интернете рекомендуется убедиться, что сетевой экран включен и настроено автоматическое обновление.

3. Внимательно относитесь к выбору браузера

Браузер – это основной инструмент для выхода в интернет, он играет ключевую роль в обеспечении безопасности в интернете. Хороший веб-браузер должен быть безопасным и обеспечивать защиту от утечки данных.

4. Создавайте надежные пароли и используйте менеджер паролей

Надежный пароль помогает обеспечить безопасность в интернете. Он обладает следующими свойствами:

- Длинный: минимум 12 символов, в идеале, даже больше.
- Содержит заглавные и строчные буквы, а также специальные символы и цифры.
- Не очевидный: в пароле не используются личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного. Избегайте простых последовательностей («12345», «qwerty») – такие пароли подбираются за считаные секунды. По той же причине избегайте распространенных слов («password1»).
- Не содержит запоминающихся сочетаний клавиш.
    - Замена букв и цифр похожими символами, например, “P@ssw0rd” вместо “password”, сейчас уже не является эффективной мерой – злоумышленники умеют обходить такую замену. Чем сложнее ваш пароль, тем сложнее его взломать. Использование менеджера паролей позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.
    - Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли.
    - Кодовые фразы надежнее, если слова в них идут в неожиданном порядке. Даже если вы используете обычные слова, берите такие, которые не связаны друг с другом по смыслу, и расставляйте их нелогичным образом. Это поможет противостоять словарному подбору.
    - Используете ли вы правило, которое трудно разгадать компьютеру? Например, пароль из трех 4-буквенных слов, в

которых первые две буквы заменяются цифрами и символами. Выглядит это так: «?4ей#2ка?6цо» вместо «улейрукалицо».

5. **Используйте на устройствах последнюю версию программы безопасности**

Антивирус, обеспечивающий защиту в интернете, очень важен для сохранения конфиденциальности и безопасности. Лучшие программы интернет-безопасности защищают от различных видов атак, а также обеспечивают безопасность данных в интернете. Очень важно обновлять антивирусное программное обеспечение. Большинство современных программ обновляются автоматически, что гарантирует защиту от последних угроз интернет-безопасности.

6. **Как защитить электронную почту**

Электронная почта разработана так, чтобы быть максимально открытой и доступной и позволить людям общаться друг с другом. Недостатком такой доступности является уязвимость некоторых аспектов электронной почты. Это позволяет злоумышленникам использовать электронную почту для нарушения безопасности в интернете.

Безопасность электронной почты – это набор методов, используемых для защиты учетных записей электронной почты и переписки от несанкционированного доступа, потери и компрометации. Учитывая, что электронная почта часто используется для распространения вредоносных программ, спама и фишинговых атак, ее безопасность является важным аспектом безопасности в интернете.

Спам-сообщения – это массово рассылаемые нежелательные сообщения. Большинство провайдеров электронной почты используют алгоритмы фильтрации спам-сообщений, но, несмотря на это, спам может продолжать приходить. Чтобы избавиться от спама, можно предпринять следующие шаги:

- **Отмечать спам-сообщения как спам**. Это поможет провайдеру электронной почты улучшить фильтрацию спама. Способ отметить сообщение как спам зависит от используемого почтового клиента: Outlook, Gmail, Apple Mail, Yahoo Mail и т. д.
- **Никогда не переходить по ссылкам и не открывать вложения в спам-сообщениях**. В результате таких действий на устройство могут быть загружены вредоносные программы. По крайней мере, такие действия служат подтверждением для спамеров, что это активная учетная запись электронной почты, и стимулируют их рассылать еще больше спама.
- **Соблюдать осторожность при использовании адреса электронной почты.** Полезно иметь дополнительную временную учетную запись электронной почты, используемую исключительно для регистрации и подписки. Она должна отличаться от рабочей и от используемой для переписки с друзьями и близкими.

- **Большинство провайдеров электронной почты имеют настройки конфиденциальности**. Убедитесь, что они установлены на комфортном для вас уровне.
- **Изучить сторонние спам-фильтры для электронной почты.** Они обеспечивают дополнительный уровень кибербезопасности, поскольку электронные письма, прежде чем попасть к адресату, должны пройти через два спам-фильтра: спам-фильтр почтового провайдера и сторонний фильтр.

Слишком много спам-писем может быть признаком того, что ваш адрес электронной почты был раскрыт в результате утечки данных. В этом случае рекомендуется сменить адрес электронной почты.

Требования к размещению информации на личных страницах в соц.сети

Если вы не топ-блогер с миллионом подписчиков, то сделайте свою страницу в соцсети закрытой, то есть доступной только друзьям, а не всем, кто на нее зайдет. Топ-блогеры - чаще всего люди опытные и отлично знают, какую информацию можно выкладывать в открытый доступ, а какую - нет. И вообще готовы к последствиям своей публичности.

Не публикуйте фотографии посадочных талонов. Авиасообщение начинает возобновляться, и многие радостно публикуют на своих открытых страницах посадочные талоны на рейсы. Зачастую - со штрих-кодами, номерами рейсов и фамилиями.

Чем это опасно? Тем, что любой человек, увидевший такое фото, может при желании войти в личный кабинет и как минимум отменить билеты.

То же самое с билетами на концерты и другие мероприятия. Если в кадре засветился штрих-код - злоумышленник легко отфотошопит его, распечатает и пройдет сам.

Отпускные фото в открытом доступе - настоящая находка для домашних воришек. Фото с берега моря и подписью вроде: "Еще семь дней в этом раю!" дают вполне понятный сигнал преступникам, предупреждает полиция. От геометок в открытом доступе тоже лучше отказаться.

Столь же настоятельно не рекомендуется во всеуслышанье хвастаться новыми дорогими гаджетами и домашней техникой. Сделайте свою страницу закрытой и потом поделитесь радостью с друзьями.

Банковская карта - не тот предмет, которым стоит делиться в соцсетях со всеми желающими. Разумеется, никаких фото документов на вашей странице тоже появляться не должно. И даже если вы нашли чей-то паспорт или водительские права и хотите отыскать владельца - действует то же правило, которое гласит: нельзя. Кстати, страницы со вклеенными визами могут содержать данные о паспорте, поэтому и их "светить" может быть опасно.

Отдельно не рекомендуется публиковать на открытых страницах в соцсетях фото детей - ни своих, ни чужих. Во-первых, из интернета ничего не удалишь, и ребенок спустя несколько лет может не очень-то обрадоваться,

увидев свои снимки в открытом доступе. А во-вторых, информацией могут воспользоваться злоумышленники.

Мобильный номер сложно удержать в секрете, однако делиться им со всеми подряд тоже не стоит. Мошеннических схем, в которых используется номер сотового, достаточно много, и они постоянно совершенствуются. Рекомендуется обзавестись резервным номером для публичного пространства и отдельным, секретным номером - для родных и близких.

Сетевая безопасность

Сетевая безопасность – это набор действий, направленных на защиту работоспособности и целостности сети и данных. Она обеспечивает защиту от множества угроз и предотвращает их проникновение и распространение в сети.

Как настроить безопасность Wi-Fi роутера

Wi-Fi роутер является важным компонентом интернет-безопасности. Он проверяет весь входящий и исходящий трафик и контролирует доступ к сети Wi-Fi, а также к телефонам, компьютерам и другим устройствам. Надежность роутеров улучшилась за последнее время, но можно предпринять дополнительные действия для усиления защиты в интернете.

Изменение заданных по умолчанию параметров роутера, таких как имя и учетные данные для входа – это важный первый шаг. Это поможет сделать сеть Wi-Fi менее уязвимой для злоумышленников, поскольку в этом случае роутер находится в активном управлении.

Чтобы повысить безопасность Wi-Fi роутера, можно отключить различные функции и настройки. Такие функции, как удаленный доступ, универсальная настройка сетевых устройств (Universal Plug and Play) и настройка защищенного Wi-Fi, могут использоваться вредоносными программами. Несмотря на то, что эти функции очень удобны, их отключение повысит безопасность домашней сети.

Использование VPN в общедоступной сети Wi-Fi

Лучший способ защитить данные в интернете при использовании общедоступного Wi-Fi – это виртуальная частная сеть (VPN). Технология VPN создает зашифрованный туннель между вашим устройством и удаленным VPN-сервером. Весь интернет-трафик передается через этот туннель, что обеспечивает защиту данных. Когда вы подключаетесь к общедоступной сети с помощью VPN, другие пользователи в этой сети не могут отследить ваши действия, что обеспечивает надежную защиту в интернете.

Программное решение, обеспечивающее круглосуточную интернет-безопасность

Лучшее программное обеспечение для интернет-безопасности защищает от целого ряда угроз, включая взломы, вирусы и вредоносные программы. Комплексный продукт для обеспечения безопасности в интернете должен обнаруживать уязвимости устройств, блокировать киберугрозы до момента их распространения, а также изолировать и устранять непосредственные опасности.

Блокировка доступа к веб-камере для конфиденциальности в интернете

В результате взлома злоумышленники получают доступ к камере вашего мобильного телефона или компьютера и записывают ваши действия. Это называется “camfecting”. Количество зарегистрированных атак этого типа относительно невелико, хотя в большинстве случаев жертвы не осознают, что их камеры были взломаны, и такие случаи остаются неучтенными.

Самый простой способ заблокировать доступ к веб-камере – использовать клейкую ленту. Однако это невозможно, если регулярно приходится использовать видеоконференции для работы и для общения. Гораздо эффективнее использовать антивирус, обеспечивающий защиту веб-камеры, например, Kaspersky Internet Security. Также рекомендуется выключать компьютер или ноутбук, когда он не используется.

Блокировщики, защищающие от вредоносной рекламы

Блокировщики рекламы убирают рекламу с веб-страниц. При блокировке рекламы исчезает риск просмотра и перехода на вредоносную рекламу. У блокировщиков рекламы есть и другие преимущества. Например, они снижают количество файлов cookie, хранящихся на компьютере, повышают конфиденциальность в интернете благодаря сокращению отслеживания, экономят трафик, обеспечивают более быструю загрузку страниц и увеличивают продолжительность работы батареи мобильных устройств.

Некоторые блокировщики рекламы являются бесплатными, а некоторые – платными. Однако не все блокировщики рекламы блокируют онлайн-рекламу полностью, а некоторые сайты могут работать некорректно при включенном блокировщике рекламы. Можно настроить блокировщики рекламы так, чтобы допускался показ онлайн-рекламы с определенных сайтов.

Безопасный онлайн-банкинг и онлайн-шоппинг

Рекомендации по безопасности при онлайн-шоппинге:

- Убедитесь, что вы совершаете транзакции на защищенном веб-сайте. Его веб-адрес должен начинаться с https://, а не с http://; буква s означает «безопасный» и указывает на наличие у сайта сертификата безопасности. Слева от адресной строки также должен отображаться значок замка.
- Обращайте внимание на веб-адрес сайта. Злоумышленники могут создавать поддельные сайты с веб-адресами, аналогичными настоящим. Они часто меняют несколько буквы в веб-адресе, чтобы ввести пользователей в заблуждение.
- Избегайте предоставления финансовой информации при использовании публичных сетей Wi-Fi.

Рекомендации по безопасности при онлайн-банкинге:

- Аналогично онлайн-шоппингу, избегайте предоставления финансовой и личной информации при использовании публичных сетей Wi-Fi.
- Используйте надежные пароли и регулярно меняйте их.
- По возможности используйте многофакторную аутентификацию.

- Чтобы не стать жертвой фишингового мошенничества, вводите веб-адрес банка напрямую или используйте банковское приложение, но не переходите по ссылкам в сообщениях электронной почты.
- Регулярно проверяйте выписки по банковским счетам, чтобы выявить непонятные транзакции.
- Поддерживайте операционную систему, браузер и приложения в актуальном состоянии. Это гарантирует, что в них исправлены известные уязвимости.
- Используйте надежные решения для обеспечения интернет-безопасности, например продукты, предлагаемые «Лабораторией Касперского».

СПОСОБЫ МОШЕННИЧЕСТВА В СЕТИ

Просьбы о помощи

Схема, схожая с «благотворительным» мошенничеством, но более рабочая по сравнению с ним. Завладев данными для входа в аккаунт пользователя, мошенники рассылают списку его друзей слёзные сообщения с просьбами о помощи, обычно суммы указываются довольно приличные – от 5 до 20 тысяч рублей. Естественно, те люди, от имени которых поступают подобные просьбы, теряют доступ к аккаунту и не могут опровергнуть написанное. Доверчивые друзья перечисляют средства по номеру телефона или прямо на счёт социальной сети.

Данная схема обмана выросла из популярных в начале 21 века SMS-мошенничеств, когда рассылались тексты наподобие «Мама/папа, я попал в беду, не звони мне, положи на этот номер 300/500/1000 рублей»

Дабы не попасться на удочку мошенников, следует позвонить владельцу аккаунта и выяснить, действительно ли ему нужна помощь.

Оплата доставки

Кто же откажется от бесплатного приза? Правильно, никто. Именно этим и пользуются мошенники, рассылая по социальным сетям и почтовым адресам яркие поздравительные сообщения с текстом о том, что пользователь выиграл приз – от сладостей до смартфона или путешествия. Единственное условие для получения приза – пересылка за счёт выигравшего. Сумма обычно невелика – от 20 до 500 рублей, но после её получения, так называемые благодетели, больше не выходят на связь.

Компании, которые действительно проводят розыгрыши, не требуют платы ни за пересылку приза, ни за таможенные сборы.

Фишинг

Это кража идентификационных данных (например, ФИО, пароль и номер банковской карты). Злоумышленники пользуются невнимательностью граждан и завладевают конфиденциальной информацией путем создания сайтов-клонов, фальшивых аккаунтов в мессенджерах и соцсетях, электронной рассылки писем.

Преступники выдают себя за надежный источник в сети, вынуждая жертву передать им личные данные.

Опросы в виде SMS

Мобильные операторы иногда устраивают опросы, чтобы выяснить, удовлетворены ли абоненты условиями связи. Эту особенность переняли и мошенники, однако с одним изменением — от них опросы поступают в виде SMS, а не звонка. В сообщении мошенники просят отправить в ответ цифру, которая соответствует степени удовлетворенности абонента (от 1 до 10). Если жертва не замечает подвоха и отправляет ответ на короткий номер, с ее счета списываются деньги.

Чаще всего такие сообщения отправляется с коротких номеров "5500", "9260", "4411" и некоторых других. Важно знать, что опрос от настоящего оператора проводится только в виде звонка — никаких сообщений отправлять не нужно.