

Пароли

На этом уроке учащиеся узнают, как защитить свою информацию в Сети с помощью пароля. Мы поговорим о том, как создать надежный пароль и почему нельзя сообщать пароли другим людям. Наконец, мы обсудим, как защитить сами пароли и предотвратить несанкционированный доступ к своим аккаунтам.

Материалы

Пароли — раздаточные материалы

Основные сведения о паролях

Часть 1

Текст для преподавателя

Мы часто не задумываемся о паролях, которые используем на сайтах, в приложениях и сервисах. Однако от того, насколько надежны ваши пароли, зависит безопасность вашей информации.

Взаимодействие в группе

Предложите участникам обсудить следующие вопросы. Напомните им, что они не должны сообщать свои реальные пароли во время выполнения упражнений.

Вопросы ученикам

Сколько паролей вы используете?

Используете ли вы разные пароли для каждого из аккаунтов электронной почты и социальных сетей?

Отличаются ли они друг от друга кардинально или представляют собой вариации одного и того же пароля?

Если у вас несколько паролей, как вы запоминаете, какой из них принадлежит какому аккаунту?

Вопросы ученикам

Как часто вы забывали важный пароль?

Что вы делали, когда забывали пароль?

Что вы делали, чтобы ваши пароли было легко вспомнить?

Есть ли пароль, который вы используете каждый день?

Что случится, если без вашего ведома кто-то узнает ваш пароль?

Имеет ли значение, кто это может быть?

Какую информацию может узнать тот, кто воспользуется вашим паролем,

чтобы войти в ваш аккаунт?

Часть 2

Взаимодействие в группе

Разделите участников на пары.

Текст для преподавателя

Со своим напарником обсудите, что может произойти, если кто-то, кто хочет устроить вам проблемы, узнает ваш пароль от аккаунта в социальной сети.

Взаимодействие в группе

Дайте участникам 5 минут на обсуждение. Затем попросите их поделиться результатами.

Текст для преподавателя

А теперь обсудите в парах, что может произойти, если хакер узнает пароль от банковского счета ваших родителей или опекунов?

Взаимодействие в группе

Дайте участникам 5 минут на обсуждение. Затем попросите их поделиться результатами.

Часть 3

Текст для преподавателя

Давайте теперь поговорим о том, как хакер может узнать ваш пароль. Существует несколько способов. Один из них — социальный инжиниринг, когда злоумышленник хитростью заставляет человека поделиться паролем. Например, хакер может отправить электронное письмо, которое выглядит так, как будто оно отправлено платформой или сайтом, где у пользователя есть аккаунт. В этом электронном письме может быть ссылка, по которой человек должен перейти, чтобы войти в аккаунт со своими учетными данными. Когда это происходит, хакер узнает, какие учетные данные использовались.

Иногда злоумышленники пытаются угадывать пароли, используя распространенные комбинации вроде "пароль123", "тест" или имя и фамилию человека.

Другой способ узнать пароль — с помощью атаки методом перебора. Он

заключается в том, что хакер пытается войти в аккаунт, перебирая возможные варианты паролей. Бывает, что хакеры проводят такую атаку вручную, но чаще всего они используют компьютерную программу, которая быстро перебирает пароли. Например, это может быть список возможных паролей или набор комбинаций из букв и цифр. Программа работает, до тех пор пока не подберет правильный пароль.

Конечно, некоторые атаки этого типа более изощренные. Если у вас пароль типа "fido123" или "пароль", программа быстрее подберет его, попробовав эти варианты, прежде чем искать менее вероятные или случайные комбинации. Атака может оказаться более эффективной, если злоумышленник знает какую-то информацию о вас. Например, если хакеру известно, что вашего любимого питомца зовут Тоби, он может попробовать использовать это слово с разными цифрами на конце (например, "Тоби629" или "Тоби3020").

Принципы создания паролей

Часть 1

Вопросы ученикам

Кто знает, что такое "надежный пароль"? Зачем нужно использовать надежные пароли?

Текст для преподавателя

Надежный пароль служит хорошим защитником вашей информации. Хотя надежный пароль не является гарантией того, что ваш аккаунт не взломают, он значительно снижает эту вероятность по сравнению с более слабым паролем.

Упражнение "Создание пароля"

Вопросы ученикам

Приведите примеры слабых паролей.

1. Например: "пароль", "12345", "Привет!", дата рождения, прозвище.

Почему эти пароли не надежны?

1. Их легко может подобрать человек и/или компьютерная программа.

Как можно сделать пароль более надежным?

1. Добавить цифры, буквы в верхнем и нижнем регистрах, символы, сделать пароль длиннее, избегать распространенных фраз и слов.

Взаимодействие в группе

После того как участники запишут свои варианты, напишите инструкции на доске:

Добавьте хотя бы одну цифру.

Добавьте хотя бы один символ.

Добавьте хотя бы одну заглавную букву и одну строчную.

Пароль должен состоять минимум из 7 символов.

Пароль должно быть легко запомнить (если только вы не пользуетесь менеджером паролей).

Менеджер паролей — это сайт или приложение, которое помогает хранить и упорядочивать пароли.

Пароль не должен представлять собой одно распространенное слово или личную информацию (например, дату рождения, имя родственника и т. д.).

Не следует использовать один и тот же пароль на разных сайтах.

Текст для преподавателя

Существует два подхода к созданию надежных паролей. Первый — следовать инструкциям наподобие тех, что написаны на доске. То есть, вы пытаетесь составить пароль из трудно угадываемых элементов. Недостаток этого подхода заключается в том, что такие пароли трудно запомнить.

Надежные пароли

Текст для преподавателя

Другой подход состоит в соблюдении определенной длины пароля. Надежность пароля зависит от его длины. Пароль, который состоит из четырех или более не связанных друг с другом слов, является "крепким орешком" как для злоумышленников, так и для компьютерных программ. Кроме того, такие пароли легче запомнить.

Наконец, можно использовать оба этих метода, то есть составить пароль из четырех или более не связанных друг с другом слов и добавить символы и цифры.

Цель этих методов одна — создать уникальный пароль, который не смогут угадать или подобрать другие люди.

Текст для преподавателя

Разделите участников на пары.

Пусть они попробуют создать надежный пароль, следуя инструкциям на доске. Помните, что пароль, который сложно подобрать компьютерной программе, может оказаться не таким сложным для человека или программы со списком распространенных длинных паролей. Лист бумаги с паролем не нужно будет сдавать в конце упражнения. Не следует использовать придуманный пароль

для своего аккаунта, так как другие участники группы знают его.

Дайте участникам 5 минут. Затем попросите их назвать примеры надежных паролей. Спросите, могут ли они вспомнить записанные пароли, не глядя на них.

Одни сайты требуют, чтобы ваш пароль соответствовал некоторым (или всем) этим условиям, в то время как у других нет определенных требований. Вы также можете создать пароли с помощью строки случайно подобранных слов.

Взаимодействие в группе

Попросите участников, оставаясь в тех же парах, создать новые пароли, представляющие собой последовательность слов. Скажите им, что в пароле должно быть минимум четыре слова, потому что так он будет надежным, но в тоже же время легко запоминаемым. Дайте участникам 5 минут. Затем попросите их назвать примеры надежных паролей. Напомните учащимся не использовать в качестве примеров свои реальные пароли. Кроме того, скажите, что по окончании урока мы не собираем листы бумаги, на которых они делали записи.

Текст для преподавателя

Некоторые сайты используют многофакторную (или двухфакторную) аутентификацию для подтверждения вашей личности. Эти сайты часто используют текстовые сообщения, приложение или электронную почту для отправки вам одноразового кода, который нужно вводить вместе с паролем.

Этот метод обеспечивает более надежную защиту аккаунта. Например, чтобы войти в ваш аккаунт, злоумышленник должен не только знать ваш пароль, но и иметь доступ к приложению, устройству или электронной почте, которые связаны с вашим аккаунтом.

Защита паролей

Часть первая

Текст для преподавателя

Даже если вы создадите пароль, который будет трудно взломать, он может быть слабым по другим причинам.

Вопросы ученикам

В каких ситуациях даже надежные пароли могут считаться слабыми?

1. Вот несколько примеров: использование одного и того же пароля для разных аккаунтов, использование пароля, который содержит личную информацию, использование одного и того же пароля в течение нескольких лет, ситуации, когда вы забыли пароль.

Как часто, на ваш взгляд, нужно менять пароли?

Текст для преподавателя

Даже надежные пароли могут быть взломаны или украдены. Однако вы можете принять дополнительные меры безопасности, чтобы этого не случилось. Если на сайте произошла утечка данных, вы можете поменять пароль на нем, а также на других сайтах, где вы используете похожие пароли.

Запоминать длинные и сложные пароли непросто.

Вопросы ученикам

Считаете ли вы хорошей идеей записывать пароли на листе бумаги или хранить в файле на компьютере? Почему?

Взаимодействие в группе

Злоумышленник может найти лист бумаги или файл на компьютере. Расскажите об использовании диспетчера паролей — приложения, которое помогает хранить и упорядочивать пароли.

Часть вторая

Текст для преподавателя

Каждый день мы используем множество разных аккаунтов на разных сайтах.

Каждый раз вводить учетные данные заново может быть весьма утомительно.

Вопросы ученикам

Вы когда-нибудь использовали функцию "сохранить пароль" в браузере? Почему?

Понимаете ли вы, как сайт запоминает вас?

1. Попросите объяснить. Затем расскажите, что сайты запоминают вас по файлам cookie. Файлы cookie — это небольшие файлы, которые хранятся на вашем компьютере и помогают сайту идентифицировать вас, когда вы открываете его в очередной раз. Однако эти файлы могут также использоваться для отслеживания ваших переходов с сайта на сайт. Именно на этом основана таргетированная реклама.

Считаете ли вы безопасным сохранять пароль, если он находится на вашем собственном компьютере?

Вопросы ученикам

Используете ли вы пароль для входа на компьютер?

Что если вы захотите предоставить доступ к своему компьютеру другому человеку?

1. В этом случае, даже если при вводе пароль будет скрыт точками или звездочками, другой человек может догадаться, какой у вас пароль. То, что вы не видите пароль на экране, не означает, что пароль не может храниться где-то ещё.

Вопросы ученикам

Бывают ли ситуации, когда можно сообщать пароль другим людям? Когда? Зачем?

1. Например, пароль нужен родителям или у вас общий или семейный аккаунт на таком сервисе, как Netflix.

Бывает ли, что вы сообщаете свой пароль другому человеку? Если да, то кому и почему?

Если ваш близкий друг скажет "если ты мне друг, дай мне свой пароль", выполните ли вы эту просьбу? Почему?

Текст для преподавателя

Вы можете сообщить свой пароль кому-то, кто вам дорог. Однако помните: дружба не означает, что они могут требовать полный доступ к вашим онлайн-аккаунтам.

Подумайте как следует об отношениях с этим человеком, в том числе о том, как они могут измениться в будущем. Например, сообщить пароль родителям или опекуну — это одно, а вот лучшему другу — это совсем другое.

Вопросы ученикам

Что может произойти с вами, если вы сообщите пароль другим?

1. Злоумышленник может взломать ваш банковский счет, узнать ваши секреты или действовать от вашего имени в Интернете.

Если вы сообщите кому-то пароль от своего аккаунта, будете ли вы использовать этот аккаунт по-другому?

Вопросы ученикам

Может быть, вы не будете смотреть что-то на Netflix или не будете писать о чем-то по электронной почте, если будете знать, что у кого-то ещё есть доступ.

Взаимодействие в группе

Участники должны подумать о том, как они сами пользовались аккаунтами с общим доступом. Они должны осознать, что их действия в Интернете видны другим пользователям.

Вопросы ученикам

Если аккаунт (например, профиль в социальной сети) является вашим виртуальным вторым "я", считаете ли вы безопасным разрешать другим людям пользоваться таким аккаунтом?

Взаимодействие в группе

Обсудите, что может произойти, если другой человек будет представляться вами и отправлять сообщения вашим друзьям от вашего имени.

Вопросы ученикам

Храните ли вы пароли на своих устройствах? Почему? Как вы думаете, безопасно ли хранить пароли на телефоне или компьютере? Что может

произойти, если вы дадите другу попользоваться вашим телефоном или компьютером?

Бывает ли, что вы даете попользоваться вашими устройствами членам семьи или друзьям? Эти люди используют ваш аккаунт на этих устройствах или у каждого из них свой аккаунт?

Вы когда-нибудь использовали "публичное" устройство, например в библиотеке или в школе? На этих устройствах вы делаете то же самое, что и на собственных?

Часть третья

Взаимодействие в группе

Разделите участников на пары.

Текст для преподавателя

Пусть они вспомнят, пользовались ли они когда-то публичным компьютером, например в библиотеке или школе. И бывало ли, что они замечали, что кто-то забыл выйти из своего аккаунта до них? Попросите участников подумать, смогли бы они совладать с искушением "полазить" по чужому аккаунту?

Взаимодействие в группе

Дайте 5 минут на обсуждение. Обсудите вопросы, связанные с несанкционированным использованием аккаунтов, всей группой.

Несанкционированный доступ к аккаунту

Часть первая

Взаимодействие в группе

Внимание! Некоторые темы этого занятия уже обсуждались на уроке 1: "Основные сведения о паролях". Вы можете повторить или пропустить их.

Текст для преподавателя

Иногда, чтобы получить доступ к вашему аккаунту, человеку вовсе не обязательно знать ваш пароль или подбирать его. Если кто-то владеет достаточной информацией о вас, он может догадаться, какой у вас пароль, или убедить кого-то из ваших коллег поделиться вашей информацией. Поскольку при этом не используются какие-либо технологии, такие атаки называются "социальным взломом" или "социальным инжинирингом".

Вопросы ученикам

Поднимите руки те, кто когда-нибудь забывал пароль к сайту.

Что произойдет, если нажать "Я не помню пароль"?

1. Обычно пользователя просят ответить на контрольные вопросы, отправляют сообщение на телефон или письмо электронной почты.

На какие вопросы вы должны будете ответить?

1. Подумайте, на какие вопросы могли бы дать правильные ответы ваши друзья или знакомые? Например: "как зовут вашего питомца", "где вы родились", "какая девичья фамилия вашей матери", "как зовут любимого учителя", "как зовут вашего лучшего друга" или "какая у вас любимая спортивная команда".

Кто ещё может знать эту информацию о вас?

Как сайт может связаться с вами, если вы забудете пароль?

Кто ещё может получить доступ к вашим контактам?

Вопросы ученикам

Как незнакомый человек может узнать о вас информацию, которая позволит

правильно ответить на контрольные вопросы?

1. Публикации в социальных сетях, результаты поиска в Интернете, подбор вариантов, обращение к друзьям и т. д.

Какими могут быть публикации в социальных сетях, содержащие личную информацию?

1. Например, фото вашей кошки в Instagram с указанием ее имени в подписи, фото с геометкой или публикации о дне рождения.

Как можно узнать информацию о человеке или даже его пароли с помощью Google?

1. Если в результатах поиска можно найти групповое фото учеников девятого класса, опубликованное в школьной онлайн-газете, вы можете узнать имя учителя.

Часть вторая

Текст для преподавателя

Не следует публиковать информацию, которая может помочь ответить на ваши контрольные вопросы. Выбирайте такие контрольные вопросы, ответы на которые знаете только вы. Вы можете сами задать ответы на эти вопросы. Если ответы достаточно простые, вы можете держать их в памяти, если нет — можно доверить их программе, которая запоминает и хранит пароли.

Сайты могут связываться с пользователями по номеру телефона или адресу электронной почты, указанному в аккаунте. Если пользователь забудет пароль, сайт может предоставить ему временный пароль или ссылку, по которой можно будет перейти, чтобы сбросить пароль.

Вопросы ученикам

Как убедиться в том, что человек, запрашивающий новый пароль, не является злоумышленником?

Что если вы сообщите кому-то свой электронный адрес, связанный с вашим аккаунтом?

1. Чаще всего метод сброса пароля является безопасным, однако если вы сообщаете учетные данные к аккаунту другому человеку, вы сильно рискуете.

Текст для преподавателя

Злоумышленник может обратиться к вам напрямую и попытаться "выудить" из вас эту информацию. Например, вы можете получить электронное письмо якобы от вашего друга, родственника или сотрудника банка с просьбой сообщить важную информацию (например, дату рождения). Либо злоумышленник может взломать аккаунт вашего друга в социальной сети и отправить вам (или другим пользователям) сообщение от имени этого человека с просьбой сообщить дату или место вашего рождения. Если вы получили сообщение от друга, которое кажется вам странным, прежде всего свяжитесь с этим другом (только не через социальную сеть). Спросите, действительно ли он отправлял вам это сообщение.

Атаки, которые используют поддельные электронные письма или сайты, называются "фишингом". Они предназначены для кражи идентификационных данных. Например, злоумышленник может оформить на ваше имя кредитные карты и пользоваться ими, из-за чего у вас могут возникнуть проблемы с оформлением кредитных карт в будущем.

Информация, полученная с помощью фишинга, может позволить злоумышленнику читать ваши электронные письма, писать сообщения от вашего имени или украсть ваши деньги. Кроме того, злоумышленник может заблокировать вам доступ к аккаунту, создав новый пароль, который вы не знаете.

Задание

Раздаточный материал

Задание

Попросите участников ответить на следующие вопросы и добавить свои ответы (текст или рисунки) в раздаточные материалы урока "Пароли".

1. Каким трем советам из этого урока вы будете следовать при создании пароля?
2. Приведите пример ситуации, когда, на ваш взгляд, можно сообщить свой пароль другому человеку.
3. Назовите три способа безопасно делиться своим паролем с другими людьми.
4. Приведите три примера того, что может случиться, если ваш пароль попадет в руки злоумышленников.