kaspersky

Надежность пароля

Методические рекомендации для учителя

kaspersky

Надежность пароля

Методический материал носит рекомендательный характер, и учитель, принимая во внимание особенности класса, может изменять вопросы и дополнять задания.

Цель урока:

Сформировать знания и умения у учащихся о методах защиты личного информационного пространства на основе надежного пароля, рассмотреть различные негативные варианты утечки паролей к злоумышленникам и провести практическую работу по разработке программного кода по генерации надежного пароля.

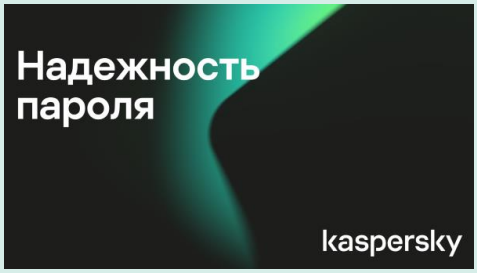
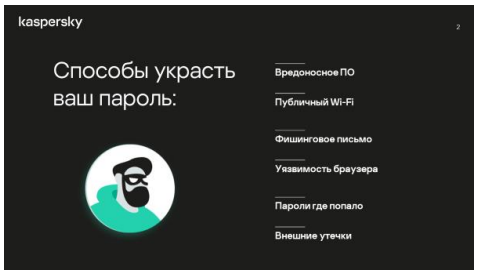
Ключевые слова:

- **Пароль**
- **Защита информации**
- **Аутентификация**
- **Менеджер паролей**

Методическое обеспечение и средства обучения:

- **Презентация**
- **Материал для учителя**
- **ПК с предустановленной средой программирования**

Таблица 1. Комментарии к каждому слайду

Слайд	Комментарии
	После приветственных слов и обозначения темы мероприятия, следует провести дискуссию с учащимися о жизненных ситуациях, при которых личный аккаунт был защищен ненадежно, какая ситуация произошла и какие пути решения были предприняты. И задаем главный вопрос мероприятия: «Какой пароль является надежным?» При этом учащиеся могут приводить конкретные примеры.
	Самые распространенные способы украсть пароль: • **Вредоносное ПО.** Существенную часть активных зловредов составляют трояны-стилеры. Они ждут, когда пользователь зайдет на какой-нибудь сайт или сервис, копируют введенный им пароль и отправляют своему владельцу. Если не пользоваться защитными решениями, то такие трояны могут годами скрываться в системе. Их трудно заметить, поскольку они тихо занимаются своим делом, не причиняя видимого вреда. Иногда киберпреступники внедряют в сайты веб-скиммеры, которые собирают всю информацию, вводимую пользователями (имена, данные учетных записей и банковских карт и т.д.). • **Публичный Wi-Fi.** Злоумышленники могут перехватить данные (в том числе пароли), отправляемые по сети,

если использовать сеть Wi-Fi без шифрования или защищенную старым протоколом WEP. Другой вариант кражи: хакер создает точку Wi-Fi с открытым доступом, используя название, похожее на существующую сеть. Не замечая разницы, пользователи подключаются к фальшивой точке – и весь их интернет-трафик оказывается под контролем злоумышленника. Избежать таких утечек можно, если внимательно проверять названия сетей, не пользоваться сомнительными точками доступа и не позволять устройствам подключаться к беспроводным сетям автоматически.

- **Фишинговое письмо.** Это один из тех подходов к краже чужих учетных данных, которые действительно рассчитаны на ошибку пользователя. В сети ежедневно появляются сотни фишинговых сайтов и тысячи рассылок, призванных заманить туда будущих жертв. У киберпреступников была масса времени, чтобы изобрести множество уловок, основанных на социальной инженерии и трюков, позволяющих им мимикрировать под легитимных отправителей.
- **Уязвимость браузера.** Нередко пароли крадут через уязвимости браузеров или через браузерные расширения. В первом случае специально созданный вредоносный код на веб-странице позволяет подсадить шпиона. А во втором случае пользователь самостоятельно устанавливает себе шпионский скрипт под видом полезного браузерного плагина или расширения. После этого, когда пользователь заходит, например, на сайт банка, этот скрипт будет перенаправлять трафик через хакерский прокси-сервер и таким образом «сливать» учетные данные.
- **Пароли где попало.** Многие до сих пор записывают пароли на стикерах и других бумажках, оставляя в местах, где их легко может увидеть посторонний. Не менее опасно записывать пароли в незащищенных текстовых файлах на своем компьютере или смартфоне, а также не рекомендуется сохранять пароли в браузере для автоматической подстановки.
- **Внешние утечки.** Все, что сказано выше, касается потери пароля на пользовательской стороне. Но утечки часто происходят и в удаленных интернет-сервисах. Это может быть интернет-магазин, социальная сеть, криптобиржа или любой другой ресурс, где при входе используется аутентификация. В результате взлома такого сайта хакеры могут получить огромную базу пользователей вместе с их паролями и другими персональными данными. При этом владельцы сайтов не всегда спешат сообщать о таких взломах. А злоумышленники тем временем обмениваются украденными базами или выставляют их на продажу в дарквебе. Специалисты по безопасности отслеживают публикации таких баз и предупреждают пользователей. Правда, иногда под видом таких специалистов высока вероятность наткнуться на мошенников.

После озвучивания возможных вариантов утраты пароля от личного аккаунта дискутируем о том, кто и как сталкивался с одним из конкретных способов. И вектор дискуссии должен

быть направлен на то, что не всегда надежный пароль может защитить информацию, а в качестве усиления защиты выступает двухфакторная аутентификация. Рассматриваем возможные ее варианты и снова проводим дискуссию о том, у кого из учащихся она подключена, что является вторым подтверждением личности пользователя и о каких технологиях им известно.

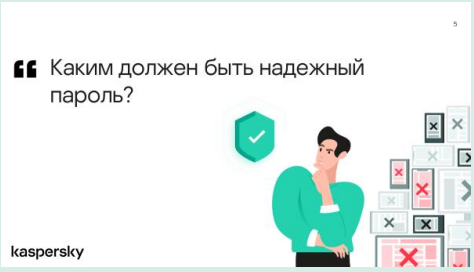
Формулируем общие рекомендации:

- Не используйте один и тот же пароль для нескольких учетных записей.
- Создавайте длинные и надежные пароли.
- Храните пароли в защищенном месте.
- Если имеется информация об утечке данных из сервисов или с сайтов, которыми пользуетесь, то сразу же меняйте пароль для доступа к ним.
- Пользуйтесь менеджером паролей.
- Используйте двухфакторную аутентификацию везде, где она доступна.

Говоря о менеджерах паролей, следует сообщить, что основной функционал таких приложений не только в генерации надежного пароля, но и в защищенности хранения информации (путем шифрования данных).

Все большая часть нашей жизни проходит в онлайне, поэтому у каждого пополняется личная «цифровая связка ключей» – от социальной сети, от банка, от почтового ящика, от любимого магазина и т.д. Поэтому очень важно, чтобы эти ключи были максимально надежны, и важнейшим условием этого является уникальность пароля для каждой из учетных записей.

Цитата специалиста Лаборатории Касперского должна натолкнуть учащихся на размышление о том, что реальная жизнь и жизнь в онлайне требуют задумываться о безопасности.



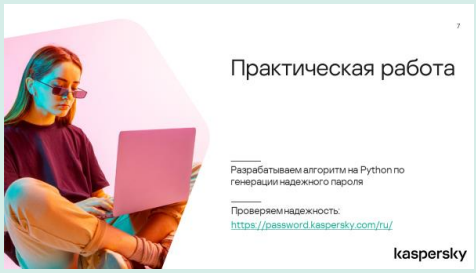
Проводим дискуссию с учащимися по вопросу: «Каким должен быть надежный пароль?»

В ходе рассуждений необходимо прийти к выводу, что длина пароля и использование различных символов (прописные и строчные буквы, цифры, символы) – это два основных критерия надежности пароля.

Предлагаем учащимся проанализировать два указанных пароля. Какой из них они будут считать надежным и почему?

С первого взгляда будет казаться, что второй пароль надежнее первого, так как в первом пароле присутствуют подряд идущие цифры и его легко можно прочитать. А у второго пароля нет какой-то закономерности выбора символов в позициях, и он содержит разнообразные буквы, цифры и символы.

На самом деле, оба пароля являются надежными. Так как первый пароль обладает большей длиной, чем второй.



Практическая работа заключается в разработке алгоритма генерации пароля на языке Python, с последующей проверкой на надежность.

Если результат выполнения алгоритма не проходит проверку, то необходимо увеличить длину получаемого пароля.

Для генерации случайного выбора из необходимых символов нужно импортировать модуль random.

Замечание: случайно сгенерированные числа и данные, полученные при помощи модуля random в Python, лишены криптографической защиты. Данный модуль порождает случайные значения на основе формулы, так что правильнее сказать, что полученные данные псевдослучайны. Но такой способ генерации удобен для многих задач.

Более подробная информация о модуле random:

https://docs.python.org/3/library/random.html

Подводим итоги занятия.

Контрольные вопросы:

- Какие требования предъявляются к надежности пароля?
- Что позволит увеличить защиту аккаунта в дополнении к паролю?
- Какие бывают способы утраты пароля?

Благодарим за внимание.

www.kaspersky.com/
www.securelist.com