**КИБЕР-ГИГИЕНА: КАК НАДЕЖНЫЙ ПАРОЛЬ ПОМОГАЕТ ПРЕДОТВРАТИТЬ УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

*При проведении данного занятия рекомендуется использовать подготовленную Национальным центром защиты персональных данных презентацию. Приведенный далее текст содержит указания на слайды, к которым относится соответствующая информация.*

**1. Введение**

*(Слайд 1)* Для того, чтобы обозначить актуальность темы, в начале занятия необходимо попросить учеников поднять руки при положительном ответе на следующие вопросы:

*”У кого на всех девайсах (телефон, компьютер и др.) и во всех социальных сетях одинаковый пароль?*

*У кого есть несколько вариантов паролей, которые вы чередуете между собой?*

*У кого для каждого девайса и соцсети есть свой пароль?“[[1]](#footnote-1)*

”Вопросы, которые были только что заданы, очень часто встречаются в опросах, посвященных кибербезопасности. Существенная часть таких опросов проводится для изучения поведения школьников в интернете, ведь именно вы пользуетесь им наиболее активно.

Проанализировав результаты ряда подобных исследований, можно отметить общую для всех опрошенных школьников особенность: даже при том, что у многих учеников разные пароли для разных девайсов и учетных записей, большинство таких паролей крайне ненадежные“.

**2.** **Теоретическая часть**

”Как вы уже, наверное, догадались сегодня мы поговорим о кибер-гигиене, то есть об обеспечении собственной безопасности в интернете. В частности, о том, как её соблюдать и что бывает, если этого не делать.

Представим, что вы – команда программистов. Вместе вам удалось найти уязвимое место в системе защиты базы данных пользователей популярной социальной сети. Логины и пароли миллионов людей оказались у вас. Далее вы загрузили эти данные в специальную программу, выбрали интересующую вас социальную сеть или сервис и запустили автоматический подбор. В случае, если в другой социальной сети или сервисе пользователем был задан точно такой же логин и пароль, как и в социальной сети, которую вам удалось взломать, по окончании такого подбора, вы получите доступ к ещё одной учетной записи того же человека.

*А теперь давайте порассуждаем. Как изменится ситуация, если у пользователя везде были разные пароли?“*

*(Слайд 2)* ”Нетрудно догадаться, что в случае, когда пароль везде одинаковый, преступникам значительно проще добраться до ваших персональных данных. Только в текущем году в сеть ”утекло“ около полутора миллиона записей, содержащих персональные данные граждан.

Поэтому сегодня мы сфокусируемся на том, что делает пароль
по-настоящему надежным. Начнем с ваших предположений.

*Как вы думаете, какой пароль мы можем назвать ненадежным? И что же такое ”надежный пароль“?“*

*(Слайд 3)* Указанные вопросы можно задать по очереди, а можно обсудить ответы на каждый из них по отдельности. Важно при этом записывать на доске все предположения учеников в две колонки – ”надежный пароль“ и ”ненадежный пароль“. В качестве подсказок для учеников можно использовать информацию из приложения 1 к занятию.

*(Слайд 4)* ”Для того, чтобы ваш пароль соответствовал большинству из требований, которые были сейчас названы, можно придумать или сгенерировать в специальных программах случайную комбинацию из букв разного регистра, цифр и символов. Однако надежный пароль совсем не обязательно должен быть сложным, главное, чтобы вы могли его запомнить.

Для этого, вы можете создать собственную ”кодовую фразу“. Кодовые фразы намного надежнее обычных паролей, потому что они, как правило, длиннее, что затрудняет их перебор.

Так, вместо того, чтобы указать в качестве пароля одно слово, выберите фразу и используйте первые буквы, цифры и знаки препинания из этой фразы, чтобы создать хороший пароль. Например:

*Фраза – ”Дважды два равно шесть“, пароль – ”Dva\*dva=6“.*

Другой вариант – создать запоминающуюся фразу из 4-7 несвязанных слов и выучить ее как строку из стихотворения. Например:

*Фраза – ”Маленький мальчик нашел цветочек“, пароль – 1Malenkiy2Malchik3Nashel4Cvetochek5.*

Для того, чтобы добавить символы к своим паролям, не усложняя их запоминание, вы всегда можете использовать текстовые смайлики. Например:

*”:-)Dva\*dva=6:-)“.*

**3. Интерактивная часть**

*(Слайд 5)* Вариант 1.

Предложите ученикам, используя ранее полученную информацию о правилах составления пароля[[2]](#footnote-2), придумать несколько максимально надежных паролей.

Вариант 2.

Следует объединить учеников в пары, раздать каждой паре одну из карточек, представленных в приложении 2, и предложить оценить степень надежности изложенных на карточке паролей. В случае, если пароли представляются ненадежными, их следует доработать.

Для проверки результата работы в обоих случаях можно воспользоваться специализированными бесплатными сервисами, доступными в интернете (например, https://password.kaspersky.com/ru/).

**4.****Заключение**

*(Слайд 6)* ”Теперь вы знаете, как создать по-настоящему надежный пароль. Никогда не поздно начать беспокоиться о своей приватности. Поэтому рекомендую проверить все свои действующие пароли и, если они недостаточно надежные, поменять их.

Если же вы используете ”правильные“ пароли для каждой учетной записи, менять их часто не требуется. Наоборот, частая смена паролей может привести к использованию менее надежных паролей или повторному использованию старых“.

|  |  |
| --- | --- |
|   | Приложение 1 к занятию”Кибер-гигиена: как надежный пароль помогает предотвратитьутечку персональных данных |

**Правила создания надежного пароля**

1. Пароль должен быть длинным – не менее 8 символов.
2. Пароль должен быть максимально уникальным, хорошо запоминаться и при этом быть надежным. Считается, что надежный пароль должен включать буквы нижнего и верхнего регистров, цифры и символы, которые в идеале должны быть расположены хаотично или неповторимым и понятным лишь владельцу учетной записи образом.
3. Воздержитесь от использования в паролях легкодоступной личной информации, такой как ваше имя, дата рождения или другие слова, с которыми вы себя часто ассоциируете (футболист, певица и т.д.), например, в социальных сетях. Злоумышленники часто используют информацию, доступную в Интернете, для подбора паролей.
4. Придерживайтесь правила: одна учетная запись – один пароль.
5. Не храните пароли на смартфоне или в браузере. Если ваше устройство будет утеряно или взломано, к сохраненным паролям могут легко получить доступ посторонние. Самый надежный способ – запомнить их наизусть.
6. Регулярно проверяйте, не был ли ваш адрес электронной почты связан с утечкой данных. В интернете есть специальные ресурсы, где это можно сделать бесплатно (например, https://haveibeenpwned.com/). Если адрес вашей электронной почты оказался среди ”слитых“ в интернет данных, немедленно измените свои пароли к учетным записям, где этот адрес используется в качестве логина.
7. Используйте двухфакторную или двухслойную аутентификацию везде, где это возможно. Она обеспечивает многофакторную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж – это логин и пароль, второй – специальный код, приходящий по SMS или электронной почте.
8. Проверить надежность пароля можно с помощью одного из специализированных бесплатных сервисов, доступных в интернете (например, https://password.kaspersky.com/ru/).

|  |  |
| --- | --- |
|   | Приложение 2 к занятию”Кибер-гигиена: как надежный пароль помогает предотвратить утечку персональных данных“ |

|  |  |
| --- | --- |
| Hello\_world123456789hahaha007parolKatePetrova1985 | KNONCEpTErEDor123456Masha\_Pertova\_140514Hello\_world123456789 |
| Sobakabezhalapopolu:)X9u|@o[C^32%=Eqwerty4563987658 | undUcHInsiLKINpassword4chelovekachertilichertezh1111111111 |

1. Здесь и далее курсивом выделены вопросы, требующие ответов аудитории. [↑](#footnote-ref-1)
2. При наличии возможности можно раздать каждому ученику ”Правила создания надежного пароля“, изложенные в приложении 1 к занятию. [↑](#footnote-ref-2)