Муниципальное автономное общеобразовательное учреждение

«Средняя общеобразовательная школа №63» г. Перми

**Методическая разработка классного часа**

**«Информационная безопасность»**

 **Безопасность аккаунта**

**Автор-разработчик:**

Марущак Джамиля Наилевна,

учитель музыки

классный руководитель

evgenui1976@yandex.ru

Пермь,2022

**Занятие на тему
«Безопасность аккаунта»**

На сегодняшний момент, возрос уровень требований к обеспечению безопасности жизнедеятельности детей в учебных учреждениях, ведь безопасность – это не только сумма усвоенных знаний, а умение правильно вести себя в различных ситуациях, самостоятельность и ответственность за свое поведение, и прежде всего одна из категорий формирования ценностного отношения к своему здоровью.

     Именно все дети должны получить систематизированную информацию о безопасном поведении на улице, дома, в быту, в сети Интернет и приобрести необходимые навыки такого поведения, тем более в каникулярное время, когда большую часть времени дети находятся одни дома.

   Полученные «теоретические» знания ребёнок должен пропускать через продуктивную деятельность и затем реализовывать в играх и повседневной жизни за пределами школы.

   В ходе своей работы я пришла к выводу, что эффективнее всего в течение учебного года одну неделю в четверть посвящать этой работе целиком с целью «погружения» ребёнка в данную проблему. Все виды внеурочной деятельности ребёнка в течение недели объединены одной темой. Полученные знания детей в рамках «тематической недели», закрепляются затем в течение всего года в играх, конкурсах, досугах. Метод проектов позволяет вовлекать детей в самостоятельный поиск, учит прогнозировать последствия поведения и деятельности в окружающем мире, овладевать практическими умениями, участвовать в творческой деятельности.

 Положительной стороной проектирования являются рисунки, поделки, газета – они позволяют слить воедино слово и образ, представление и понятие, что способствует расширению и закреплению знаний детей ОБЖ. Хочу поделиться одним из занятий, посвященном безопасности детей в сети Интернет.

**Возраст: 4-5 класс**

**Цель:** формирование общепринятых норм поведения в сети Интернет через повышение грамотности обучающихся в вопросах безопасности личных данных.

**Задачи:**

* познакомить со способами защиты личных данных в интернете, которые помогут избежать взлома паролей, потери аккаунта, отслеживания действий в сети и обеспечат безопасность онлайн-общения;
* систематизировать знания о безопасной работе в сети Интернет;
* сформировать у учащихся навыки безопасной работы в интернете на основании имеющегося у них опыта;
* сформировать критическое отношение к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
* воспитать дисциплинированность, культуру общения.

**Ход занятия:**

**На доске буквы: Ь О З А О П Б Е С Т Н С**

 12 9 3 6 4 5 1 2 7 11 8 10

Переставить буквы, и вы прочитаете тему нашего занятия.

**Ведущий:**

Он знает всё и даже больше,

И к нам на помощь поспешит.

Любой вопрос, пусть очень сложный,

Мгновенно с лёгкостью решит.

Плетёт свою он паутину,

Хотя, по сути, не паук.

Он видит всё.

 Вы догадались?

А ну-ка, что это за друг? (Ответ: Интернет)

Чтобы переписываться по электронной почте, общаться в социальной сети или делать покупки в интернет-магазине, нужно сначала там зарегистрироваться. Другими словами, завести учётную запись, или аккаунт.

У любого аккаунта есть логин и пароль. Логин — это имя пользователя в системе, а пароль — ключ, который открывает к ней доступ. Ваш логин могут знать многие. В почте, например, логин — это одновременно и электронный адрес. А вот пароль должны знать только вы и никто больше.

Ввод пароля — это не единственный способ пройти проверку на входе. Иногда вместо пароля используют токен — специальное USB-устройство, которое нужно вставить в компьютер, чтобы авторизоваться. Пароль также могут заменять биометрические данные: отпечатки пальца, голос, сетчатка глаза.

Чтобы усилить защиту, сайт или сервис может требовать вместе с паролем что-то ещё. Например, одноразовый код, который приходит по смс или создается в специальном приложении. Такой код сложно своровать, да и смысла в этом нет — ведь действует он всего один раз. Авторизация с двойной защитой — паролем и одноразовым кодом — называется двухфакторной аутентификацией.

Звучит серьёзно, правда? Но и охота на учётные данные тоже идёт серьёзная

1. **Как взламывают аккаунты**

Есть разные способы. Кто-то применяет самый банальный метод перебора, или, как его ещё называют, брутфорс. В этом мошенникам помогают программы-боты. Они просто перебирают символы или, чтобы было быстрее, проверяют пароли по специальным словарям для взломщиков. В них входят популярные пароли типа 1234, qwerty и обычные слова и фразы из разных языков. Увы, многие люди используют для своих аккаунтов такую вот ненадёжную защиту.

Другой способ получить пароль — перехватить его. Для этого подходят, например, вай-фай сети в кафе или парках. Публичный вай-фай очень часто устроен так, что в нём ваши данные может увидеть любой, кто подключится к сети. А подключиться может кто угодно — в том числе и злоумышленник.

Ещё мошенники нередко «восстанавливают пароль» вместо пользователей. Например, по секретному вопросу. Найти на него ответ бывает совсем несложно — в той же соцсети. Вспомните об этом, если захотите рассказать друзьям ВКонтакте о своей любимой компьютерной игре, а потом сделать это секретным вопросом в почте. Да и вообще — лучше выбирать для восстановления доступа более надёжные способы. Скажем, код в смс.

Наконец, самые хитрые добиваются того, что пользователи сами, по доброй воле, отдают им свои логины и пароли. Все, что для этого нужно, — выдать себя за какой-нибудь известный сервис или организацию. Допустим, прислать письмо от имени банка и попросить у человека пароль от онлайн-кабинета — якобы для решения технических проблем. Или показать окошко авторизации, нарисованное в стиле популярного сайта — мол, у вас новое сообщение, авторизуйтесь, чтобы прочитать. Такой способ обмана называется фишингом, то есть рыбалкой по-английски. Пользователь, ничего не подозревая, клюёт на удочку, и его личные данные отправляются прямиком к самозванцам.

1. **Как защитить аккаунт**

**Вход в квартиру мы защищаем дверью с замком.** А вход в свой аккаунт — паролем. Как и замок на двери, пароль должен быть надёжным.

Что это значит? Во-первых, пароль должен быть длинным, не меньше 8-10 символов. Во-вторых, сложным, то есть содержать разные типы символов — цифры, большие и маленькие буквы, специальные знаки вроде звездочки, решетки, знаков вопроса или восклицания. И в-третьих, пароль должен быть небанальным. Не надо использовать в нем свое имя, адрес, дату рождения — будьте уверены, злоумышленники знают этот приём. Обычные слова или удобные сочетания клавиш (в ряд, крестом) тоже не подойдут — они давно есть в словарях для программ-взломщиков.

**Ставьте на разные двери разные замки**. Электронная почта, интернет-магазин, социальная сеть — пароли от всех этих сервисов должны быть разными. Конечно, запомнить сразу много паролей трудно, особенно если все они правда надёжные. Но записывать их на листочках или в телефоне все равно не надо. Лучше придумайте себе правило и чуть-чуть меняйте по нему пароли для разных сервисов. На крайний случай пригодится менеджер паролей, который будет помнить их вместо вас. А вам останется запомнить только один пароль — от менеджера. Но помните, что если уж мошенники до него доберутся, то получат в свои руки сразу всё.

**Важно не только то, какой пароль вы используете, но и где вы его вводите.** Про опасность открытых вай-фаев вы уже слышали, но стоит повторить еще раз: не вводите личные данные в сети, которая открыта для всех желающих. Потому что в числе этих желающих могут оказаться мошенники. Будьте аккуратны также и с чужими устройствами, даже если доверяете их владельцу. Друг, в гостях у которого вы решили проверить почту, ваш пароль не украдет. Зато это может сделать вирус, который тайком пробрался к нему на компьютер. Если вы все же воспользовались чужим компьютером, не поленитесь почистить за собой историю и сохранённые пароли в настройках браузера.

Не забывайте про фишинг. Чтобы не попасться на удочку мошенников-фишеров, проверяйте адреса страниц. Обращайте внимание на слово перед последней точкой в адресе — это и есть настоящее название страницы. Сайт мейл-точка-яндекс-точка-ру будет принадлежать Яндексу, а вот мейл-точка-яндекс-6451-точка-ру — уже нет.

Кроме того, проверяйте, защищает ли сайт вашу информацию. Если адрес начинается с эйч-ти-ти-пи-эс и в адресной строке стоит значок замка, значит, сайту можно доверять — он передаёт все данные в зашифрованном виде. В адресах фишинговых сайтов вы такого не увидите, потому что заниматься шифрованием ваших данных мошенникам вовсе незачем. От неприятностей, увы, никто не застрахован

1. **Что делать, если взломали**

Допустим, вы ввели логин и пароль от почты на каком-то сайте, а потом поняли, что он фишинговый. Вас ещё не взломали, но данные уже скомпрометированы — они попали к злоумышленникам, которые теперь могут использовать вашу почту, как угодно. Что делать в такой ситуации? (ответы ребят)

 Самое главное — не волноваться и первым делом сменить пароль. Если вы использовали его на нескольких сервисах — сменить и там тоже.

Потом привяжите к своему аккаунту актуальный номер мобильного, если он ещё не привязан. Это помешает мошенникам поменять ваш пароль, потому что код восстановления придёт не им, а вам на телефон. Удалить ваш номер у них тоже не получится — ведь код подтверждения, опять же, получите вы, а не они.

Другая ситуация: на подозрительных сайтах и в открытых сетях вы пароль не вводили, другим людям его не передавали, а с вашей почты вдруг пачками посыпались странные письма. Или вы заметили, что ваш ящик открывают с незнакомых компьютеров — в Яндекс.Почте это можно проверить по айпи-адресам в журнале посещений. Тут, скорее всего, поработала вредоносная программа. А значит, сменой пароля и привязкой телефона уже не обойдёшься — нужно лечить компьютер. Скачайте антивирус и проверьте систему. Если один антивирус у вас уже стоит, попробуйте ещё один — который может провести проверку без установки на устройство.

1. **Итог. Рефлексия.**

В следующем задании вы сможете найти слова, о которых мы сегодня говорили на нашем занятии.

Решить филворд на тему «Безопасный аккаунт» (онлайн, аккаунт, контент, телефон, трафик, спам, хостинг, браузер, троллинг, гугл).



Рефлексия

 - я нашел(а) все слова филворда, и тема мне понятна

- я нашел(а) больше половины слов филворда, и не до конца мне понятна тема

- я нашел(а) меньше половины слов филворда, и мне не понятна тема

Интернет ссылки:

<https://www.kaspersky.ru/resource-center/definitions/what-is-internet-security>

<https://ppt-online.org/713494>

<https://dzen.ru/video/watch/62700b2c035e7c47c209318d?f=d2d>