**МОБУ ООШ – детский сад д.Абдуллино**

 **2015**

**Тема: Безопасность в интернете**

**Дата: 30.10.15**

**Цели уроков:**

1. Систематизация знаний в области использования интернета.
2. Формирование навыков безопасного использования интернета.
3. Распознавание и реагирование на интернет-угрозы.

**Задачи уроков:**

* Систематизирование знаний детей в области интернет-безопасности по направлениям:
	+ раскрытие персональных данных;
	+ мошенничества, в т.ч. мобильные, заражение компьютера и мобильных устройств;
	+ общение в сети;
	+ общая компьютерная грамотность.
* Связь навыков повседневного использования интернета и электронных устройств с правилами безопасности. Формирование у детей навыков безопасного использования интернета на основании имеющегося у них опыта.
* Повышение уровня осведомленности детей о наиболее актуальных интернет-угрозах ( с учетом возраста аудитории, региона, других факторов).
* Формирование навыков и осознанных подходов к противодействию интернет-угрозам.
* Показ важности взаимодействия детей с учителями и родителями, особенно в критических и неприятных ситуациях

**Безопасность в интернете**

**1. Общая безопасность в интернете**

Интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем

информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги,

отправляем документы для поступления в вузы и делаем многое другое. Вместе с

тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать

их.

**Какие опасности могут поджидать в интернете**

В первую очередь это действия мошенников, которые хотят получить финансовую

или иную выгоду. Мошенники могут использовать самые разные инструменты и

методы — например, вирусное программное обеспечение (или «вирусы»),

поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным

записям в социальных сетях и на почтовых сервисах.

**Вирусы**

Вирусы могут распространяться с помощью вложенных файлов, ссылок в

электронных письмах или в соцсетях, на съемных носителях, через зараженные

сайты. Сообщение с вирусом может прислать как посторонний человек, так и

знакомый, но уже зараженный участник социальной сети или почтовой переписки.

Зараженными могут быть сайты, специально созданные в целях мошенничества,

или обычные ресурсы, но имеющие уязвимости информационной безопасности.

Рекомендации

• Используйте антивирусное программное обеспечение с обновленными

базами вирусных сигнатур.

• Не открывайте вложенные файлы или ссылки, полученные по электронной

почте, через социальную сеть или другие средства связи, не

удостоверившись, что файл или ссылка не содержит вирус.

• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru),

так как злоумышленники часто используют похожие имена сайтов, чтобы

ввести жертву в заблуждение (например, www.yadndex.ru).

• Обращайте внимание на предупреждения браузера или поисковой машины

о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требование

перевести деньги или отправить смс, чтобы снять блокировку компьютера.

**Получение доступа к аккаунтам в социальных сетях и на других сервисах**

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы,

например, в социальных сетях, на почтовых и других сервисах. Украденные

аккаунты они используют, в частности, для распространения спама и вирусов.

Мошенники могут получить доступ к учeтной записи жертвы следующими

способами:

• Заставить жертву ввести свои данные на поддельном сайте.

• Подобрать пароль жертвы, если он не сложный.

• Восстановить пароль жертвы с помощью «секретного вопроса» или

указанной при регистрации электронной почты.

• Перехватить пароль жертвы при передаче по незащищенным каналам

связи.

Как правило, для кражи личных данных используются фишинговые сайты. Фишинг

(от англ. **fishing** — рыбная ловля, выуживание) — вид интернет-мошенничества,

целью которого является получение доступа к конфиденциальным данным

пользователей — логинам и паролям. Злоумышленники создают фишинговые

сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои

логины и пароли, не понимая, что сайты поддельные.

Рекомендации

• Используйте сложные пароли (они состоят как минимум из 10 символов,

включают буквы верхнего и нижнего регистра, цифры и специальные

символы, не содержат имя пользователя и известные факты о нем).

• Никому не сообщайте свой пароль.

• Для восстановления пароля используйте привязанный к аккаунту

мобильный номер, а не секретный вопрос или электронную почту.

• Не передавайте учетные данные — логины и пароли — по незащищенным

каналам связи (не защищены, как правило, открытые и общедоступные wi-fi

сети).

• Внимательно проверяйте доменные имена сайтов, на которых вводите

учетные данные.

**Памятка для детей**

Как уберечь компьютер от заражения вирусом

• Используйте антивирусное программное обеспечение с обновленными

базами вирусных сигнатур.

• Не открывайте вложенные файлы или ссылки, полученные по электронной

почте, через социальную сеть или другие средства связи, не

удостоверившись, что файл или ссылка не содержит вирус.

• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru),

так как злоумышленники часто используют похожие имена сайтов, чтобы

ввести жертву в заблуждение (например, www.yadndex.ru).

• Обращайте внимание на предупреждения браузера или поисковой машины

о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требования

перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные

• Используйте сложные пароли (они состоят как минимум из 10 символов,

включают буквы верхнего и нижнего регистра, цифры и специальные

символы, не содержат имя пользователя и известные факты о нем).

• Никому не сообщайте свой пароль.

• Для восстановления пароля используйте привязанный к аккаунту

мобильный номер, а не секретный вопрос или электронную почту.

• Не передавайте учетные данные — логины и пароли — по незащищенным

каналам связи (не защищены, как правило, открытые и общедоступные wi-fi

сети).

• Внимательно проверяйте доменные имена сайтов, на которых вводите

учетные данные.

• Не вводите пароли от важных учётных записей, когда подключены к

общественной Wi-Fi-сети.

Как не попасться на удочку смс-мошенников

• Не отправляйте смс на незнакомые телефонные номера, за оправку таких

смс могут взимать плату.

• Переводите деньги только на известные телефонные номера.

• Не вводите телефонный номер на незнакомых сайтах.

Как избежать мошенничества при платежах

• Помните, что банки и платежные сервисы никогда не просят сообщать — ни

по почте, ни по телефону — пароль, пин-код или код из смс.

• Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька

или банковской карты.

• Храните банковскую карту в надежном месте.

• Не держите записанные пароли и коды рядом с картой.

• Заведите отдельную карту для покупок в интернете.

• Используйте для покупок в интернете только личный компьютер.

• Регулярно обновляйте антивирусную защиту компьютера.

• Старайтесь делать покупки в известных и проверенных интернет-магазинах.

• Перед подтверждением оплаты убедитесь, что в адресной строке браузера

указан протокол https. Только этот протокол обеспечивает безопасную

передачу данных.

• Подключите в банке услугу уведомлений по смс, чтобы оперативно

получать сведения о совершенных транзакциях.

• Сохраняйте документы об оплате услуг и доставке товаров, полученные по

электронной почте.

• Регулярно просматривайте в интернет-банке историю выполненных

операций по вашим картам.