«Безопасность в интернете для школьников на современном этапе»

Безопасность в Интернете может включать в себя несколько понятий – компьютерная безопасность , кибербезопасность.

Классификация интернет преступлений достаточно многообразна. Это мошенничество с благотворительностью, подарочными картами , кликбейт и другие.

Аферисты преследуют единственную цель — обманным путем получить деньги или имущество. Они умеют располагать к себе, играть на эмоциях и чувствах, запугивать. Среди них есть психологи, специалисты по финансам, экономике, страхованию и т.д.

Мошеннические схемы направлены на совершение транзакции (безналичного перевода) денежных средств на счет преступников. Злоумышленники в интернете становятся все изобретательнее и в условиях пандемии новой коронавирусной инфекции, социальной нестабильностью, информационными вбросами, фейками и другими информационными составляющими.

Проведенный опрос на уроке ОБЖ состоял из 4 вопросов

Делитесь ли вы личной информацией в интернете?

Скачиваете ли файлы из непроверенных источников?

Подвергались ли ваши данные попыткам кражи/взлома?

Используете ли вы антивирусные программы при работе в интернете?

Учащиеся могли ответить положительно или отрицательно.

Опрос помог мне понять, что большинство учащихся 10-го класса делятся личными данными в интернете (около 67% опрошенных)

Опрошенные не скачивали данные из непроверенных источников (61% не делали этого)

Почти никого, к счастью, не пытались взломать

Но, 28% опрошенных стоит установить антивирус, 72% уже сделали это.

Что же можно порекомендовать обычному школьнику для обеспечения своей компьютерной безопасности?

1. Установите антивирусные программы

Для защиты от вирусов существуют антивирусы. Важно не просто пользоваться ими, но и периодически обновлять их базы данных, ведь создатели вредоносных программ то и дело запускают в интернет свои новые разработки. 2. Используйте сложные логины и пароли

Логин в виде имени, фамилии и пароль типа 1234 или QWERTY – не лучшая идея. Если кто-то всерьез решит похитить вашу конфиденциальную информацию, он расколет такую «защиту» в два счета. Хороший логин и пароль – это сложная комбинация, в которой используются заглавные и строчные буквы, цифры и символы. 3. Не передавайте конфиденциальные сведения

Не пересылайте пароли, логины, паспортные данные, ПИН-коды и прочую подобную информацию в мессенджерах, чатах или по электронной почте. Не делайте этого, даже если ваш собеседник утверждает, что он – представитель службы безопасности банка. 4. Ограничьте информацию о себе в интернете

Многие социальные сети позволяют настраивать список тех, кто может просматривать ваш профиль и отправлять сообщения.

Можно, например, сделать так, чтобы писать вам было разрешено только тем, с кем у вас подтверждена дружба – и при этом, конечно, стоит убедиться, что вы имеете представление о каждом своем онлайн-друге.

5. Не открывайте подозрительные письма

Прежде чем открыть письмо, пришедшее на электронную почту, прочитайте заголовок и посмотрите, с какого адреса оно было отправлено. Если тема вам неинтересна, заголовок составлен с грубыми ошибками, адрес представляет собой хаотичное нагромождение символов или напоминает название вашего банка, но с переставленными буквами, сразу отправляйте письмо в корзину. И никогда не открывайте файлы .exe в подозрительных письмах.

6. Не переходите по подозрительным ссылкам

Даже если всплывающая ссылка обещает что-то очень интересное и выгодное, лучше не кликать на нее. Если ссылку прислал вам знакомый, причем без каких-либо комментариев, сначала уточните, что он имел в виду. Возможно, его взломали, и теперь мошенники используют его профиль для рассылки вредоносных программ.

7. Не устанавливайте сомнительные приложения

Есть два безопасных источника приложений:

официальные магазины, созданные Apple, Google, Microsoft и другими подобными компаниями;

официальные сайты компаний, разработавших приложения.

Установка приложений из других источников, в том числе различных ломаных и пиратских версий, может закончиться тем, что вам придется тщательно чистить компьютер или телефон от вирусов.

8. Блокируйте подозрительных пользователей

Если у вас появились подозрения, что тот, кто пишет вам в интернете – мошенник, смело блокируйте его. Это не займет много времени, но поможет сберечь нервы и денежные средства. Многие из мошенников знают, как вызвать жалость, обмануть, запугать и заговорить человека. Поэтому с такими людьми лучше даже не вести бесед и смело отправлять в черный список. Также у нас есть удобная услуга «Безопасный режим», подключив которую, нежелательные сообщения, спам и интернет-подписки будут блокироваться автоматически – обратите внимание.

Библиография

https://ru.wikipedia.org/wiki/Интернет-мошенничество

https://ru.wikipedia.org/wiki/Интернет#Ключевые\_принципы

https://ru.wikipedia.org/wiki/Сетевой\_этикет

https://ru.wikipedia.org/wiki/Компьютерная\_безопасность

Интерне́т // Русский орфографический словарь / Под ред. В. В. Лопатина. — 4-е. — М.: АСТ-пресс книга, 2013. — С. 243. — ISBN 978-5-462-01272-3.

Большая российская энциклопедия : [в 35 т.] / гл. ред. Ю. С. Осипов. — М. : Большая российская энциклопедия, 2004—2017.