«Согласовано»
председатель профкома:
_____/Мазинова Г.И./
«__07__» ___10_____ 2020г.

«Утверждаю»
директор МОУ «ВГЛ»
_____/Захарова С.М./
«__07__» ___10_____ 2020г.

Инструкция № 5.52

Инструкция
для обучающихся по обеспечению информационной безопасности причиняющей вред их здоровью и развитию при использовании сети «Интернет»

1. **В интернете не стоит переходить по ссылкам и нажимать кнопки во всплывающих сообщениях, которые кажутся подозрительными.**
   Не загружайте приложения, которые кажутся вам странными или находятся на неизвестном сайте. Не уверены, что письмо настоящее? Задайте себе следующие вопросы: не подозрительный ли у отправителя адрес электронной почты? Используется ли безличное приветствие? Много ли орфографических ошибок? Пытается ли автор письма создать ощущение срочности?

2. **Для защиты личной информации придумайте надежный пароль и никому его не сообщайте. Для каждого ресурса стоит использовать уникальные логины и пароли.**
   Чтобы безопасно хранить разные пароли для разных учетных записей, используйте менеджер паролей и убедитесь, что для каждой учетной записи используется сложный пароль, состоящий минимум из 10 символов — заглавных и строчных букв, чисел и специальных знаков.

3. **Никогда не предоставляйте секретные сведения, например, номер счета или пароль в ответе на сообщение электронной почты или в социальных сетях.**
   Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на предложения о сделке, которые слишком хороши, чтобы быть правдой, на сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

4. **Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка рядом с адресной строкой, который обозначает безопасное соединение**
   Прежде чем публиковать что-то в Интернете, спросите себя: хотите ли вы, чтобы ваши работодатели, клиенты и родственники знали это? Даже такие данные, как статус ваших отношений или домашний адрес, которые могут показаться безобидными, могут быть использованы во вред, если их увидят не те люди.

5. **Для безопасности общения в социальных сетях оставляйте как можно меньше данных о себе и избирательно подходите к предложениям о дружбе.**
   Не все, кого вы встречаете в Интернете, являются теми, за кого себя выдают. Киберпреступники часто создают поддельные профили в социальных сетях, чтобы вступать в переписку с доверчивыми пользователями и обирать их электронные кошельки — или делать еще что похуже.
   Перед просмотром входящих писем на электронном ящике, проверьте адрес отправителя. Подозрительные письма смело отправляйте в спам, особенно если в таких письмах содержатся прикрепленные файлы.
   Не открывайте подозрительные письма странного происхождения, не поддавайтесь на содержащиеся в них сомнительные предложения лёгкого заработка, не высылайте никому пароли

от ваших аккаунтов, не открывайте прикреплённые к письмам подозрительные файлы и не переходите по содержащимся в них подозрительным ссылкам.

7. **Для скачивания картинки или мелодии вам предлагают отправить смс? Не спешите! Сначала проверьте этот номер в интернете — безопасен ли он и не обманут ли вас.**
   Если вы все еще не уверены, свяжитесь с фигурирующей в сообщении компанией по официальным каналам, таким как веб-сайт или страница в социальных сетях. Всегда лучше проверить и перепроверить, чем рисковать своей безопасностью.

ПРОВЕРЕНО

специалист по ОТ _____ Власова С.Б.

«07» 10 2020г.