РОССИЙСКАЯ ФЕДЕРАЦИЯ
РОСТОВСКАЯ ОБЛАСТЬ

муниципальное бюджетное общеобразовательное учреждение г.Шахты Ростовской области «Средняя общеобразовательная школа№1»

346 517, г. Шахты Ростовской обл. ул. Достоевского 69, тел.(88636) 28-97-58, 28-85-06, факс (8636) 28-01-68, e-mail: mousoh1-shahty@mail.ru

Инструктаж для педколлектива по правилам безопасности работы в сети Интернет.

I) В последнее время участились случаи компьютерных атак, осуществляемых путём направления электронных сообщений с вредоносными вложениями на служебные и личные адреса электронной почты сотрудников органов государственной власти. Тексты писем направляются адресату с учётом специфики и сферы его деятельности, личных интересов. Адреса отправителей часто имитируют адреса известных российских предприятий, организаций и новостных агентств.

Примеры:
1.Сообщения на телефон с неизвестного номера, типа «срочно пойди по ссылке».
2.Сообщение с номера, имитирующего номер организации. Например, от Сбербанка не с 900, а с номера 9000.
3.Сообщения на электронную почту о взломе вашего аккаунта в социальной сети.
4.Сообщения типа «вы выиграли 1000000 рублей», «специальное предложение по кредиту», «чтобы похудеть нужно каждый день…», «с вами хочет познакомиться…».

Рекомендации:
1.Внимательно изучайте e-mail отправителя. Если сообщение от организации, сравни с e-mail*ом* на официальном сайте.
2.Не открывайте и удаляйте подозрительные сообщения.
3. В настройках своей электронной почты блокируйте рассылку с адресов, вызывающих у вас подозрения.

II. Сейчас злоумышленники часто используют такой вид взлома как fishing. Под видом необходимости регистрации на сайте или установки дополнительного ПО для корректной работы они незаконно собирают личную информацию о пользователи с цель получения доступа к его паролям, учётным записям, операциям по банковским картам.

Пример:
1.Десятки сайтов пытаются выдать себя за официальный сайт https://online.sberbank.ru/ с целью получить ваши логин и пароль от личного кабинета, и доступ к вашим финансовым средствам.
2.На тысячах сайтах для скачивания файлов требуют ввести ваш номер телефона и адрес электронной почты. В дальнейшем они используются для рассылки спама и сообщений с вредоносными вложениями. При запуске они передают информацию о вас злоумышленникам, также они могут заблокировать ваши устройства или удалённо ими управлять.
3. Всплывающие окна и реклама с провокационным содержанием «Путин женился», «Ванга предсказала», «Секрет вечной молодости» «Обмануть интернет-казино» и т.д. и т.п. Они активируют запуск вредоносного ПО или переход на сайты его распространяющие.

Рекомендации:
1.Проводите финансовые операции только на сайтах с доверенным соединением.

2.Регистрируйтесь только на сайтах официальных организаций, предоставляющих информацию о своём местоположении, контактах, ответственных лицах.
3.Никогда не вводите свои паспортные данные, СНИЛС и реквизиты прочих официальных документов. Исключение только для официальных государственных сайтов, таких как https://www.gosuslugi.ru/.
4.Если на сайте много баннеров, всплывающих окон т рекламы, лучше покиньте его.

III.Часто имеет место злоумышленный подлог при распространении информации и файлов.

Пример:
Вместо файла, который вы хотели скачать скачивается иной файл, который выдаёт себя за web-установщик. Довольно часто под видом torrent-файлов.

При его запуске, на который вы сами даёте согласие по запросу системы, может быть установлено какое угодно вредоносное ПО.

Рекомендации:
Всегда проверяйте загруженные файлы антивирусом. Послу установки ПО его или место его размещения тоже рекомендуется проверить.

IV.Серьёзную опасность представляет установка вместе с программным обеспечением дополнительного нежелательного и вредоносного ПО. Например, различных вирусных рекламных модулей типа candy, которые без вашего ведома изменяют закладки, стартовые страницы, поисковые системы, вашего браузера.

Пример:
Многие официальные разработчики бесплатного ПО в свои сборки добавляют данные вирусные программы. Даже такие крупные и известные фирмы как Google и Yandex стремятся по умолчанию навязать различные toolbar*ы* и прочие вебслужбы.

Рекомендации:
1.Загружайте ПО с официальных сайтов разработчиков.
2.Внимательно знакомьтесь с условиями его предоставления и лицензионным соглашением. При установке вы часто сами даёте доступ к своим файлам, разрешаете рекламу и пр.
3.При установке ПО обязательно заходите в настройки инсталлятора и убирайте ненужные вам модули.

Общие рекомендации.

1.Настройте блокировку рекламы в своём браузере и почтовом клиенте вручную или используя специальные программы типа Adblock.

2.Желательно использовать отдельные почтовые клиенты типа Mozilla Thunderbird или OperaMail. В них хорошие настройки безопасности, нет рекламы, можно хранить переписку на сервере или на своём устройстве.

3. Используйте браузер с конфиденциальными настройками, постарайтесь отключить слежение, загрузку cookie файлов, не отмечайте без необходимости своё географическое положение, отключите автоматическую рассылку данных работы вашего браузера даже его разработчикам. Регулярно очищайте историю посещений и загрузок.
3. Не используйте оборудование и специальные электронные приложения со своего места работы для личной переписки и внеслужебного обмена файлами.

4. Используйте антивирус с актуальными базами.

5. Следите за своим интернет трафиком. Вы должны чётко понимать, что вы скачиваете и какую информацию передаёте.

6. Будьте осмотрительны, никто кроме вас, ни одна технология не защитит от человеческой халатности.