«Прокуратура Баймакского района обращает внимание на соблюдение безопасности компьютеров в целях профилактики киберпреступлений»

Вслед за развитием информационных технологий, их проникновением во все сферы жизнедеятельности человека закономерно растет количество регистрируемых компьютерных инцидентов.

Законодательством Российской Федерации предусмотрена ответственность, в том числе уголовная, за совершение противоправных деяний в сфере высоких технологий (ст.ст. 272-274.1 УК РФ).

Несмотря на то, что без компьютеров уже невозможно представить современную жизнь, многие люди до сих пор не осознают огромные риски, связанные с постоянным взаимодействием с технологиями.

Прокуратура района обращает внимание как физических, так и юридических лиц на необходимость соблюдения так называемой «компьютерной гигиены».

Компьютерные вирусы – одна из самых старых форм программного обеспечения, предназначенного для нанесения вреда, но их способность избегать обнаружения и самовоспроизводиться означает, что эти программы всегда будут вызывать беспокойство.

Понимание того, что вирус может сделать с Вашим компьютером, - это первый шаг к обеспечению безопасности Вашей системы и защите вашей семьи от атак.

Вирус также может направлять веб-браузер пользователя на нежелательные сайты или даже заблокировать компьютер и попросить выкуп за его разблокирование.

В самых тяжелых случаях вирус может повредить важные компьютерные файлы, что сделает систему практически бесполезной.

Существует несколько нехитрых правил «компьютерной гигиены», следование которым поможет минимизировать вероятность поражения компьютера:

1) Приобретите и пользуйтесь платным антивирусом. Отсутствие антивируса резко увеличивает вероятность заражения компьютера, а бесплатные продукты обычно имеют сильно урезанный функционал.

2) Используйте антивирус. Простой установки антивируса бывает недостаточно для эффективного противостояния угрозам.

Необходимые меры при работе с антивирусом:

• Регулярное обновление.

• Регулярный запуск проверки системы.

• Проверка антивирусом подключаемых к компьютеру носителей информации (флешек, жестких дисков и т.д.), а так же файлов, скаченных из интернета.

3) Устанавливайте только знакомые Вам программы, взятые из известных источников.

4) Не используйте пиратское программное обеспечение.

5) Работая в интернете, обращайте внимание на то, на каком именно сайте вас просят ввести пароль, номер телефона или совершить какое-либо действие. Злоумышленники часто пользуются неопытностью, подменяя адреса известных сайтов, предлагая скачать вирусы под видом обновлений программного обеспечение.

6) Используйте длинные и сложные пароли, сочетание цифр, строчных и заглавных букв. Это усложнит злоумышленникам доступ к Вашей информации.

Обеспечение защиты от киберпреступлений может занять довольно продолжительное время, но всегда того стоит. Соблюдение таких правил безопасной работы в Интернете, как воздержание от загрузок из неизвестных источников и посещения сайтов с низкой репутацией — это здравый смысл в рамках предотвращения киберпреступлений. Внимательное и бережное отношение к своим учетным и персональным данным может также существенно поспособствовать защите от злоумышленников.

Помощник прокурора района

юрист 3 класса Л.Н. Шафеева