«Компьютерная гигиена», как способ профилактики преступных посягательств с использованием IT-технологий

Валуйская межрайонная прокуратура обращает внимание физических и юридических лиц на необходимость соблюдения компьютерной безопасности в условиях активного развития современных информационно-коммуникационных технологий, которые порождают новые угрозы общественной безопасности.

С ростом количества телекоммуникационных устройств и пользователей информационных сетей увеличивается число потенциальных жертв, а также возрастают возможности эксплуатации сети «Интернет» для совершения противоправных действий.

Влияние на увеличение количества преступлений с использованием IT-технологий оказывает активное развитие новых форм платных услуг и сервисов, а равно использование при расчетах цифровых средств платежей.

Посредством сети «Интернет» мы делаем покупки, храним на ПК важные данные и иную личную информацию. Полностью отказаться от использования гаджетов не получится, но возможно научится пользоваться ими безопасно.

Когда говорим о безопасности в Интернете, напрашивается сравнение с личной гигиеной человека, то есть чтобы более или менее безопасно «путешествовать» по Сети, надо соблюдать элементарные правила, которые должны войти в привычку у каждого, кто хочет минимизировать риски, и по возможности не сталкиваться с проблемами и конечно не стать жертвой злоумышленников в современном мире высоко развитых информационных технологий.

Главной целью указанных выше лиц является получение денежных средств, в связи с чем необходимо осторожнее относиться к регистрации на сомнительных сайтах и по возможности придумывать сложные пароли, применяя цифры, символы и буквы разного регистра, одновременно следив при этом, чтобы пин-коды не повторялись.

Злоумышленники, назовем их «киберпреступниками» (мошенники) прежде всего используют вредоносные программы, которые позволяют не только читать сообщения и копировать документы с устройства жертвы (потерпевшего), но также активировать микрофон и камеру. В целях избежания вторжения вредоносного программного обеспечения в компьютер пользователя необходимо соблюдать ряд правил, которые помогут не стать жертвой такого рода преступления.

Во-первых, необходимо отказаться от скачивания программ из недостоверных источников, установить антивирус и постоянно обновлять программное обеспечение до последней версии. При этом приобретать и пользоваться желательно платным антивирусом, поскольку его отсутствие резко увеличивает вероятность заражения компьютера, а бесплатные продукты имеют сильно урезанный функционал.

Во-вторых, ограничить доступ мобильных приложений к камере, микрофону и геоположению, в случаях, когда это не ограничивает работу используемых программ.

В-третьих, не переходить по ссылкам, которые имеются в письмах, присланных от неизвестных пользователей, а также по рекламным баннерам, которые имеются почти на всех сайтах, а также по возможности ограничить скачивание информации из сети «Интернет».

Работая в Интернете обращать внимание на то, на каком сайте просят ввести пароль, номер телефона или совершить какое-либо действие. Если есть сомнения и неуверенность — лучше обратиться за помощью к специалисту. Злоумышленники часто пользуются неопытностью, подменяя адреса известных сайтов, предлагая скачать вирусы под видом обновлений программного обеспечения.

Ни в коем случае не сообщать данные банковской карты, иные личные данные неустановленным лицам, при