**Как защитить себя от «кибермошенников»**

Самыми распространенными преступлениями в сфере компьютерной информации (киберпреступлениями) являются неправомерный доступ к компьютерной информации (ст.272 Уголовного кодекса РФ), распространение вредоносных компьютерных программ (ст.273 Уголовного кодекса РФ), а также мошеннические действия, совершенные с использованием электронных средств платежа (ст.159.3 Уголовного кодекса РФ).

Жертвами мошенников в сети «Интернет» становятся не только начинающие пользователи, но и юридически грамотные люди.

Основными признаками того, что Вас пытаются обмануть, являются очень заманчивые и привлекательные предложения, такие как: высокий заработок в «Интернете» за час работы, низкие цены в интернет – магазинах.

Должно насторожить любое виртуальное мероприятие, которое требует вложения денежных средств, предоплаты.

При покупке товаров настораживающими факторами являются отсутствие возможности курьерской доставки и самовывоза товара, отсутствие у продавца или магазина «истории», неточности или несоответствия в описании товаров, излишняя назойливость продавца или менеджера.

**Чтобы не стать жертвой мошенников рекомендуем следовать следующим правилам:**

1. Не доверяйте непроверенным сайтам знакомств, заработка, азартных игр, лотерей, тотализаторам.

2. Если на сайте нет юридического адреса, контактных телефонов, обратной связи, то не предоставляйте свои персональные данные, банковские сведения.

3. Не направляйте SMS-сообщения на короткие номера, указанные в инструкции по разблокировке и защите от вирусов.

4. Создавайте сложные пароли там, где есть доступ к Вашим данным и денежным средствам, пользуйтесь обновляемой проверенной антивирусной программой.

5. При совершении покупок в сети «Интернет» предварительно ознакомьтесь с информацией о магазине, отзывами о его работе, инструкцией по возврату и обмену товара. Обратите внимание на дату создания сайта по дате регистрации домена. Проверить данные об организации можно на сайте Федеральной налоговой службы России, используя ИНН и ОГРН. Помимо этого, следует с помощью поиска посмотреть «черный список интернет – магазинов».

6. Будьте аккуратны и внимательны при работе с электронными кошельками и банк-клиентами на сомнительных сайтах, а также при проведении операций на чужих компьютерах.

Важно помнить, что преступление всегда легче предотвратить, чем вернуть похищенное. Воспользуйтесь этими советами по предупреждению киберпреступлений, которые позволят вам обезопасить себя от преступных посягательств.

По сообщению прокуратуры Опаринского района