«Прокуратура Каширского района разъясняет: «Как обезопасить себя от преступлений в сфере информационных технологий или киберпреступности?».

Преступления в сфере информационных технологий включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

В наше время практически у каждого человека, живущего на Земле, имеется в собственности мобильный телефон, а также компьютер или ноутбук, которые подключены к всемирной глобальной сети «Интернет». С их помощью многие совершают онлайн - покупки или попросту привязывают свою банковскую карту к социальной сети, при этом, не задумываясь о своей безопасности.

Опасность пользования такими устройствами заключается не только в возможности их кражи, но и в возможности кражи личных персональных данных человека, которые можно использовать в различных преступных целях. Преступления, связанные с хищением личных данных, с помощью которых преступник может совершить кражу денежных средств, которые находятся на ваших личных счетах в различных банках.

Наиболее распространенным видом мошенничества является «телефонное мошенничество».

Данный вид преступления заключается в том, что злоумышленник вводит гражданина в стрессовую ситуацию по средством телефонного звонка.

Ситуации бывают разные. Иногда злоумышленник придумывает историю, связанную с совершением им ДТП или иным преступлением, за которое ему необходимо заплатить сотруднику полиции денежные средства - взятку, для того, чтобы откупиться. Причем, злоумышленник говорит, что если он не откупиться от сотрудника полиции, то его «посадят» в тюрьму. Именно слова о том, что их сына или дочь «посадят» в тюрьму, и вводят граждан в стрессовую ситуацию. Так же злоумышленник будет пытаться уговорить Вас не отключать мобильный телефон, пока вы находитесь в пути к ближайшему банкомату или терминалу. Ввиду этого, они идут на условия мошенников, и переводят им денежные средства на указанный счет банковской карты или лицевой счет сим - карты.

Есть ряд простых общих рекомендаций:

1. Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Установите и обязательно обновляйте антивирусные программы.
2. Проверяйте информацию о состоянии счетов, зачислении или списании денежных средств с них, в достоверных источниках, закажите выписку в банке, получите консультацию специалиста банка.
3. Никому не сообщайте персональные данные, в том числе пароли и коды доступа. Не храните данные карт на компьютере и в смартфоне.

Расследованием преступлений в сфере информационных технологий занимаются органы полиции. Если вы стали жертвой киберпреступления, следует обратиться в органы полиции.

Правовая справка:
Что такое киберпреступность?
Законодатель относит к киберпреступлениям неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ), неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст.274.1 УК РФ). Статьями 159.3 и 159.6 УК РФ предусмотрена уголовная ответственность за различные виды кибермошенничеств.

Максимальные санкции за совершение перечисленных преступлений предусматривают наказание в виде лишения свободы сроком от 5 до 10 лет.