Прокуратура Промышленного района г. Самара разъясняет

«Преступления в сфере информационных технологий, их виды и противодействие»

Помощник прокурора Промышленного района г.Самары Юрченко К.А.

К преступлениям в сфере информационных технологий можно отнести как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов возбуждающих межнациональную и межрелигиозную вражду и т.д.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Согласно положениям Уголовного кодекса Российской Федерации под преступлением в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Ответственность за совершение указанных преступлений предусмотрена главой 28 Уголовного кодекса Российской Федерации.

Так, к рассматриваемой категории преступлений, в соответствии с Уголовном кодексом Российской Федерации, относятся преступления в сфере компьютерной информации:

- 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 и распространение порнографии (ст. 274 УК РФ).

Кроме того, 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.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия.

В настоящее время, практически нет человека, который не использует мобильный телефон, а так же компьютер или ноутбук, с подключением к всемирной глобальной сети «Интернет». Часто, не задумываясь о своей безопасности, мы совершаем онлайн - покупки или привязывают свою

банковскую карту к социальной сети, но опасность использования таких устройств не ограничивается только в возможностью их кражи, присутствует также постоянная опасность возможность кражи личных персональных данных человека, которые можно использовать в различных преступных целях. Преступники, получившие доступ к Вашим личным данным, может совершить кражу денежных средств, которые находятся на ваших личных счетах в различных банках.

На сегодняшний день, наиболее распространенным видом мошенничества является «телефонное мошенничество». Такие преступные деяния совершаются путем введения злоумышленником гражданина в стрессовую ситуацию по средством телефонного звонка.

Так, например, 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, одной из распространенных схем киберпреступников в последние годы стал «Вишинг» – это вид мошенничества, при котором злоумышленники под любым предлогом вынуждают нас предоставлять конфиденциальные данные в «наших собственных интересах», то есть искусственно создается ситуация, требующая помощи от специалиста.

Цель мошенников под любым предлогом извлечь секретную личную информацию о кредитке. Для получения доступа к конфиденциальным данным владельца мнимые помощники используют телефонную связь как в автоматизированном режиме, так и напрямую от мнимого «операциониста» банковского сектора. Во многих случаях в течение дня нам постоянно начинают звонить на мобильник с незнакомого номера. Как только мы отвечаем на звонок, нам сразу сообщают важную информацию о возникших проблемах с нашей картой, например, что она заблокирована, а служба безопасности банка предотвратила попытку несанкционированного списания. Затем звонящий предлагает помощь в сложившейся ситуации, на которую многие из нас соглашаются. Нас убеждают в срочном решении возникшей ситуации, пока еще не все деньги украдены. Очень последовательно мошенники стараются получить от нас всю личную информацию о кредитке, присылают новые пароли и ПИН коды в СМС-уведомлениях. Успокаивающим голосом «банковские работники» предлагают различные возможные варианты защиты. Догадаться о том, что любезный помощник на другом конце провода является мошенником не всегда легко, но в любом случае это возможно. Изначально можно поблагодарить за бдительность и узнать должность, инициалы звонившего сотрудника кредитной организации и предпринять попытку дозвониться по горячей линии. Использовать для выяснения сложившейся ситуации лучше другой свой номер, потому что на сегодняшний день у вымогателей существуют технологии, позволяющие перенаправлять все последующие звонки на телефонное устройство мошенников.

Помимо изложенного, есть еще 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.

Схем мошенничества с кредитками много, и преступники постоянно придумывают новые. Чтобы использование банковских карт было не только удобным, но и безопасным, помните: самое дорогое в современном мире – это информация. Отдать персональные сведения, сведения о кредитке посторонним – это все равно, что отдать свой кошелек. При возникновении сомнения, правильным действием с Вашей стороны будет обратиться в любое ближайшее отделение банка либо обратиться к сотрудникам банка в контактный центр по телефонам круглосуточной помощи клиентам.