Сеть Интернет, являясь крупнейшим средством обмена информацией, в то же время порождает возможность осуществления противоправных деяний, связанных с использованием информационных технологий.

Сеть Интернет, являясь крупнейшим средством обмена информацией, в то же время порождает возможность осуществления противоправных деяний, связанных с использованием информационных технологий.

В последнее время число преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий, возрастает. Новые технологии все чаще выступают средством совершения самого широкого круга преступлений. Наиболее распространены хищения денежных средств, мошенничества, кражи с банковского счета и иные преступления. Не исключаются также факты коррупции, вымогательств, вовлечения несовершеннолетних в различные категории преступлений и многое другое.

В связи с этим, чтобы избежать негативных последствий для себя и своих близких, в особенности несовершеннолетних, необходимо быть предельно бдительными и помнить основные правила безопасного поведения и общения посредством информационно-телекоммуникационных технологий.

Памятка о том, как не стать жертвой кибермошенников.

1. Как защитить свой компьютер от вредоносных программ.

Вредоносные программы способны самостоятельно, то есть без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия: от вполне безобидных «шуток» (типа «гуляющих» по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

Рекомендации по обеспечению безопасной работы в Интернете:

· Установите современное лицензионное антивирусное программное обеспечение. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы

· Устанавливайте новые версии операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов

· Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять

· Регулярно выполняйте резервное копирование важной информации. Подготовьте и имейте в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой

· Используйте сложные пароли, не связанные с вашей жизнью

· Расширение файла – это важно! Особую опасность могут представлять файлы со следующими расширениями: *ade, *adp, *bas, *bat; *chm, *cmd, *com, *cpl; *crt, *eml, *exe, *hlp; *hta, *inf, *ins, *isp; *jse, *lnk, *mdb, *mde; *msc, *msi, *msp, *mst; *pcd, *pif, *reg, *scr; *sct, *shs, *url, *vbs; *vbe, *wsf, *wsh, *wsc.

2. Рекомендации о том, как уберечься от мошенничества с банковскими пластиковыми картами.

· Никому и никогда не сообщать ПИН-код карты

· Выучить ПИН-код либо хранить его отдельно от карты и не в бумажнике

· Не передавать карту другим лицам – все операции с картой должны проводиться на Ваших глазах

· Пользоваться только банкоматами не оборудованными дополнительными устройствами

· По всем вопросам советоваться с банком, выдавшим карту

· Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций

· Поставьте лимит на сумму списаний или перевода в личном кабинете банка

· Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно

· Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка

3. Рекомендации о том, как уберечься от телефонных sms-мошенников

Мошенники знают психологию людей. Они используют следующие мотивы:

üБеспокойство за близких и знакомых.

üБеспокойство за свой телефонный номер, счёт в банке или кредитную карту.

üЖелание выиграть крупный приз.

üЛюбопытство – желание получить доступ к SMS и звонкам других людей

Наиболее распространенные схемы телефонного мошенничества:

- Обман по телефону: требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

- SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.

-Телефонный номер - «грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.

- Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи: Вас просят приобрести карты экспресс-оплаты и сообщить коды либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

-Простой код от оператора связи: предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства с Вашего счёта.

- Штрафные санкции и угроза отключения номера: якобы за нарушение договора с оператором Вашей мобильной связи.

-Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку. Услуга, якобы позволяющая получить доступ к SMS и звонкам другого человека.

Рекомендации:

· Не общайтесь с посторонними людьми по телефону и не сообщайте номера своих банковских карт, коды доступа, смс - сообщения которые поступают к вам на телефон.

· Перед тем как перевести денежные средства на номер сотового телефона лица, которое сообщает Вам, что он Ваш родственник и попал в трудную ситуацию – свяжитесь с родственниками по достоверно известным Вам телефонам и уточните информацию

· Если Вам сообщили, что Ваша карта заблокирована обращайтесь в отделение банка оператору, не выполняйте указания человека, представившегося оператором.

· По возможности не используйте телефон, на котором подключено приложение «Мобильный банк», так как Ваш телефон может быть заражен вирусом, который в дальнейшем без Вашего ведома переведет денежные средства с банковской карты на чужой счет.

Чтобы не стать жертвой преступников, необходимо следовать определенным правилам:

1. Если получен звонок или сообщение в социальной сети с просьбой о срочной денежной помощи для знакомого или родственника, не стоит принимать решение сразу. Необходимо проверить полученную информацию, связавшись со своими родными и знакомыми.

2. Никогда и никому не сообщайте трёхзначный код на обратной стороне Вашей банковской карты (CVV), это ключ к Вашим деньгам.

3. Нельзя сообщать никому личные сведения, данные банковских карт и СМС-пароли, которые могут быть использованы злоумышленниками для неправомерных действий.

4. Если по телефону Вас просят набрать комбинацию цифр в банкомате, прекратите разговор. Никогда не выполняйте действия с банкоматом «под диктовку» другого человека.

Необходимо помнить, что злоумышленники могут представиться сотрудниками банка, правоохранительного органа, учреждения здравоохранения и обращаться к Вам по имени и отчеству. Однако только мошенники будут просить сообщить реквизиты банковской карты, смс-пароль (код), CVV-код Вашей карты. В каждом таком случае необходимо завершить разговор.

Сотрудники банка также не предлагают:

· установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, для удаления вирусов с мобильного устройства);

· перевести денежные средства на «защищенный счет»;

· включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.

Если Вы стали жертвой преступника, необходимо незамедлительно обратиться в органы внутренних дел с соответствующим заявлением лично либо позвонить по телефонам 102 или 112. В заявлении следует максимально подробно рассказать о всех обстоятельствах события. Также следует принять меры к блокировке банковской карты.