Профилактика правонарушений в сфере информационной безопасности

Телефонные вирусы

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета. Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

Методы борьбы:

- Не устанавливайте приложения из неизвестных источников!
- Проверяйте разрешения, которые запрашиваетустанавливаемое приложение
- Не переходите по ссылкам с неизвестных номеров и почтовых ящиков

Мошенничество с банковскими картами

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации.

Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ: Чтобы ограбить Вас, злоумышленникам нужен лишь номер Вашей карты и ПИН-код. Как только Вы их сообщите, деньги будут сняты с Вашего счета.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Не торопитесь сообщать реквизиты вашей карты! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.

Как защититься от мошенников

Никогда и никому не сообщайте ПИН-код Вашей карты.

Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами.

Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.
Немедленно блокируйте карту при ее утере
Набирая ПИН-код, прикрывайте клавиатуру рукой.
В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.
Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком – он обязан предоставить консультационные услуги по работе с картой.
В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ

1. АНТИВИРУСНЫЕ ПРОГРАММЫ – ВАШИ ПЕРВЫЕ ЗАЩИТНИКИ

Установите антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы.

2. ОБНОВЛЕНИЯ – ЭТО ПОЛЕЗНО И БЕЗОПАСНО

Отслеживайте появление новых версий операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки.
Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

3. НАСТРОЙТЕ СВОЙ КОМПЬЮТЕР ПРОТИВ ВРЕДОНОСНЫХ ПРОГРАММ

Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети.

4. ПРОВЕРЯЙТЕ НОВЫЕ ФАЙЛЫ .

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.

5. БУДЬТЕ БДИТЕЛЬНЫ И ОСТОРОЖНЫ

По возможности, не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их.
При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной

отправке вируса, немедленно проверяйте компьютер антивирусной программой.

6. РЕЗЕРВНОЕ КОПИРОВАНИЕ – ГАРАНТИЯ БЕЗОПАСНОСТИ

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