Осторожно, мошенники!

Банковские технологии уже прочно обосновались в онлайн - сегменте. Это позволяет не стоять в очередях, а из любого места, где есть доступ в «ИНТЕРНЕТ» осуществлять платежи с банковской карты, в связи с чем, стало стремительно развиваться мобильное мошенничество.

Виды мобильных мошенничеств:

1) Забыли отключить мобильный банк при смене сим-карты!!!

При получении банковской карты, клиентам обычно подключают и услугу «Мобильный банк». Кто-то им пользуется, кто-то просто смотрит СМС - уведомления о своих доходах/расходах.

Часто при смене сим-карты, люди забывают написать заявление в банке с просьбой «отключить» данную услугу в результате чего, оператор мобильной связи через некоторое время выпускает новый экземпляр сим-карты с тем же абонентским номером. Далее, «новый владелец» ранее принадлежащего Вам, абонентского номера, получает СМС - уведомления о движении денежных средств по вашему банковскому счету. Кроме этого, он также получает возможность с помощью СМС - команд переводить денежные средства с ваших счетов.

2) Мобильное заражение!!!

Пользователи мобильных устройств работающих на операционной базе «АНДРОИД», «iOS» и др., устанавливают программу, которая содержит в себе «вредоносный файл».

В этом случае, помимо «заражения вашего телефона», вредоносный файл может «автоматически», рассылать уведомления всем абонентам из вашей адресной книги, с различными ссылками. Перейдя по ссылке из сообщения, заражается и другое мобильное устройство. Далее, этот вредоносный файл получает доступ к вашему «Мобильному банку», после чего самостоятельно осуществляет перевод ваших денежных средств на счета злоумышленников, электронные кошельки, и номера мобильной связи, при этом как показала практика, вредоносный файл блокирует поступления на ваш абонентский номер СМС – уведомления о движении денежных средств по вашим счетам.

4) Изменение телефонного номера для мобильного банка!!!

Примерно год назад появился этот вид мошенничества.

Многие люди пользуются «досками бесплатных объявлений» на сайтах бесплатных объявлений, а именно, размещают там информацию о продаже чего-либо.

Мошенники звонят по объявлению. Далее, в ходе телефонного разговора, сообщают о том, что готовы внести всю сумму за продаваемый предмет путем, онлайн перевода, тем самым пробуждают дикий интерес к себе со стороны продавца. Далее, злоумышленники сообщают о том, что у них по той или иной причине не получается совершить онлайн перевод и под различными предлогами просят продавца пройти к банкомату, вставить свою карту и произвести определенные комбинации на клавиатуре банкомата. В результате чего, заинтересованный продавец, совершает сказанные комбинации на клавиатуре Банкомата, в результате чего подключается услуга «Мобильный банк» к абонентскому номеру злоумышленника. Результат - Продавец теряет деньги со счета своей банковской карты либо сберегательного счета.

5) Звонок из службы безопасности!!!

В этом случае, на Ваш мобильный телефон поступает звонок и человек, позвонивший Вам, представившись сотрудником службы безопасности, сообщает о том, что ваши банковские счета взломаны, либо в ваш личный кабинет «Интернет банка», осуществлен несанкционированный доступ. Далее злоумышленник, просит предоставить ему номер банковской карты. Естественно в большинстве подобных случаев люди не раздумывая, выполняют все действия, которые им говорит злоумышленник, так как обеспокоены состоянием своих денежных средств и воспринимают полученную информацию в серьез. Далее, по наработанной схеме, злоумышленник, имея номер

банковской карты человека, получает доступ к личному кабинету «Интернет банка» и распоряжается денежными средствами человека в своих личных интересах.

Возникает вопрос, как не стать жертвой мошенников?

Чтобы не стать жертвой мобильного мошенничества, необходимо соблюдать несколько простых правил:

- Не используйте ваш мобильный телефон для доступа к Интернет-банку;

Как промежуточный вариант, можете с одного телефона (планшета) заходить Интернет-банк, а на второй (где отсутствует доступ в Интернет) получать банковские СМС - уведомления.

- Если вы потеряли или перестали пользоваться сим - картой, то отключите на ней «Мобильный банк»;

- Никому нельзя сообщать информацию, напечатанную на обеих сторонах вашей банковской карты.

- Установите на смартфон/планшет антивирусную программу.

- Устанавливайте приложения только из официальных источников. Это Google Play для Android устройств и AppStore для устройств Apple (iPhone / iPad).

- Не производите в банкомате с картой никаких действий по рекомендациям чужих людей.

Надеюсь, данная информация, поможет Вам, не стать жертвой мошенничества.

Следователь СО ММО
МВД России «Сарапульский»
Александр Ахмадуллин