Предупрежден, значит вооружен!

Стали бы вы делиться информацией о своем благосостоянии с посторонними людьми или собственноручно доверять все свои деньги неизвестным? Согласитесь, такое представить трудно. Однако, порою это происходит. Низкая осведомленность граждан о совершаемых способах мошенничества, чрезмерная доверчивость, обман и давление со стороны злоумышленников, все это приводит к потери своих денег.

Представьте такую ситуацию. На ваш телефон поступает звонок, и неизвестное лицо, обращаясь к вам по имени и отчеству, сообщает, что является официальным представителем банковской сферы, сотрудником службы безопасности банка или другой службы, призванной обеспечить безопасность ваших счетов.

Можете ли вы таким образом определить, что человек на том конце провода действительно тот, за кого себя выдает, даже если вы слышите характерные посторонние шумы делового офиса? Навряд ли.

Далее звонящий сообщает вам, что кто-то пытается взломать вашу банковскую карту и списать денежные средства, или уже совершает переводы. В результате приостановки несанкционированных операций все ваши счета заблокированы или это срочно требуется сделать. Для чего вам необходимо назвать неизвестному: данные вашего личного кабинета, анкетные данные (чтобы сравнить их), данные банковской карты, срок действия и код безопасности, расположенный на обороте карты, а также коды из СМС-сообщений, приходящие на ваш телефон.

Запомните! Ни один сотрудник какого-либо действующего банка не будет звонить вам по данному поводу, и спрашивать коды и пароли.

Так, в ОМВД обратился 66-летний житель Зеленограда, с заявлением о мошенничестве. На принадлежащий ему мобильный телефон позвонил неизвестный, который представился сотрудником одного из банков и сообщил, что неизвестные лица пытаются перевести денежные средства в сумме 6 000 рублей с его банковской карты, и что на телефоне клиента выявлен вирус. Для предотвращения снятия денежных средств, необходимо пройти полную проверку на вирусы. Для этого неизвестный попросил сообщить ID телефона, номер и данные банковской карты. После того, как заявитель передал требуемую информацию, с имеющихся в пользовании заявителя банковских карт различных банков, были списаны денежные средства в общей сумме около 200 000 рублей.

Следователем СУ УВД Зеленограда по данному факту возбуждено уголовное дело по ст. 159.3 УК РФ.

Помните, как в детстве родители предупреждали нас о том, что общаться с посторонними людьми, пытающимися узнать у вас конфиденциальную информацию, нельзя ни в коем случае! Почему они это делали? Они хотели предотвратить беду, которая могла бы последовать после таких откровений. Однако, почему же сейчас, став взрослыми, мы забываем об этой мере предосторожности?

Что следует делать, в случае если к вам поступает аналогичный звонок:

- не сообщайте данные своих банковских счетов, а так же CVC-код, находящийся с обратной стороны карты;

- не передавайте пароли, приходящие на ваш телефон в СМС-сообщениях;

- не сообщайте данные личных кабинетов Интернет-страниц обслуживающих банков;

- не подключайте приложения или ссылки для проверки вирусов, присланные неизвестными;

- не выполняйте под диктовку неизвестного набор клавиш телефона или банкомата;

- обратитесь лично в офис банка, обслуживающего ваши счета, для решения данного вопроса.



