Как не стать жертвой мошенников: основные правила безопасности

В связи с участившимися случаями мошенничества с использованием интернет-банков рекомендуем:
— использовать сложный пароль блокировки экрана, входа в аккаунт в социальных сетях и мессенджерах, качественную антивирусную программу;
— не входить в банковские приложения, используя отпечаток пальца или функцию распознавания лица;
— не хранить в телефоне логин и пароль от входа в мобильный банкинг;
— не хранить в телефоне реквизиты карты: номер, срок действия, проверочный код и ПИН-код карты;
— избегать входа в систему мобильного банкинга с чужих устройств;
— при утрате телефона немедленно обратиться в банк для блокировки карты, а также в офис мобильного оператора для блокировки SIM-карты;
— не переходить по ссылкам из SMS-сообщений, даже если в сообщении утверждается, что оно из банка;
— отключать функцию отображения текста входящих SMS- уведомлений на экране заблокированного телефона.
Кроме того, в случае поступления сообщений с просьбой о помощи от одного из знакомых или родственников необходимо связаться с ним по телефону и уточнить отправлял он это сообщение или нет. Предпринимать какие-либо действия пока человек не подтвердит лично, что ему необходима помощь, не стоит. Тем более ни в коем случае нельзя сообщать реквизиты своей карты, трехзначный код на оборотной стороне, срок действия, пароль из смс – уведомлений посторонним лицам.