**Способы защиты от интернет-мошенников**

Анализ криминогенной обстановки свидетельствует о ежегодном увеличении на территории округа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

В подавляющем большинстве они связаны с хищением денежных средств  со счетов граждан посредством интернет-банкинга.

Для обеспечения безопасности банковских вкладов нужно соблюдать ряд простых правил.

* Ни при каких обстоятельствах нельзя сообщать третьим лицам, в том числе представляющимся сотрудниками кредитных организаций и правоохранительных органов, полученных в СМС-сообщениях и push-уведомлениях кодов безопасности для подтверждения финансовых операций, логины и пароли от личных кабинетов в мобильных приложениях банков.
* Не следует поддаваться на уговоры о перечислении различных комиссий и страховок, якобы необходимых для получения банковских услуг, переводе денег для обеспечения их сохранности на «безопасный» счёт.
* Необходимо помнить, что злоумышленники с помощью IP-телефонии могут изменить свой абонентский номер на иной, в том числе соответствующий официальным телефонам органов государственной власти и банков.
* Доступ к данным счетов и банковских карт, с использованием которых в дальнейшем похищаются деньги, может быть получен преступниками путём направления СМС-уведомлений, якобы от имени банка, с заманчивыми предложениями, к примеру об оформлении кредита на выгодных условиях, и гиперссылкой, по которой потерпевший переходит на интернет-ресурс, по оформлению и содержанию дублирующий официальный сайт банка. Вводимые на таких интернет-страницах сведения становятся доступны мошенникам.
* При попытках неправомерного доступа к находящимся на счетах денежным средствам, поступлении подозрительных звонков и уведомлений надлежит немедленно обратиться с устным или письменным заявлением в любой отдел органов внутренних дел, а также, при необходимости блокировки операций по расчётным счетам, к официальным представителям кредитных учреждений.