Предупреждение преступлений в сфере информационно-коммуникационных технологий

Развитие информационно-телекоммуникационных технологий сопровождается ростом количества преступлений, совершаемых дистанционно с использованием телефона или сети «Интернет».

Распространенной схемой телефонного мошенничества являются случаи, когда мошенник обращается от лица сотрудников правоохранительных органов (полиции, прокуратуры и т.п.) либо «служб безопасности банка». Зачастую преступники обращаются к гражданам по фамилии, имени, отчеству, сообщают, что в отношении них либо их близких родственников, друзей возбуждено уголовное дело, и им необходимо получить данные для аутентификации в системах дистанционного банковского обслуживания, сведения о совершенных по карте операциях или любую другую информацию.

Получая персональные данные гражданина, злоумышленники осуществляют переводы, совершают покупки с его счета в банке. Преступники могут убедить потерпевших самостоятельно перечислить на подконтрольные им счета свои деньги для прекращения уголовного преследования.

Иногда абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер не доступен, положи на него определенную сумму и перезвони». После пополнения счёта телефон по-прежнему остается недоступным, при этом деньги вернуть уже невозможно.

Распространены случаи хищений денежных средств при производстве онлайн продаж. Мошенники открывают в сети «Интернет» двойники интернет-магазинов, в которых предлагается приобрести дешевые товары и воспользоваться «горячими предложениями». Завлекаемые пользователи переходят по ссылке, проходят регистрацию и вводят информацию о своем банковском счете для завершения покупки. Получив оплату, продавец пропадает или присылает совершенно иной товар.

Зачастую злоумышленники создают клоны сайтов банков. Через электронную почту или смс-оповещения приглашают пользователей пройти авторизацию. После регистрации в личном кабинете на подобном сайте, раскрытия логина и пароля получают допуск к финансам и опустошают банковские счета.

Кроме того, распространены случаи взломов аккаунтов и рассылки через электронную почту, социальные сети просьб срочно перевести деньги.

Для предупреждения хищения денежных средств не следует передавать свои технические устройства незнакомым и малознакомым лицам, а при использовании интернет-ресурсов не переходить на сомнительные сайты. Не сообщайте указанным лицам свои персональные данные, а также информацию о банковских картах и счетах, не берите по инициативе третьих лиц кредиты на своё имя и не переводите свои денежные средства либо кредитные на счета звонящих Вам мошенников.

Будьте бдительны при общении по телефону и в сети «Интернет». Прокурор, следователь, сотрудник полиции, работник банка при необходимости должен лично вызвать гражданина.

Заместитель прокурора района А.В. Жидких