**«Савеловский межрайонный прокурор г. Москвы разъясняет».**

**Способы защиты для граждан и организаций от преступлений в сфере информационных технологий.**

Если в отношении Вас совершено преступление указанной категории, эффективность его расследования зависит от своевременности обращения   
в компетентные правоохранительные органы.

У организаций, которые работают с данными клиентов, есть системы логирования – хранение информации о том, кто, откуда и с каких адресов заходит в сервис, какими телефонами пользовался для доступа и т. д. Эту информацию важно сохранять для того, чтобы можно было восстановить цепочку действий, например, если клиенту в переписке отправили ссылку на фишинговый сайт или попытались выманить данные карты. Правоохранительные органы в случае происшествия запрашивают такую информацию.

В ситуации, когда совершенное преступление связано с хищением денежных средств, потерпевшему необходимо получить выписку из своего банка с подтверждением факта перевода денежных средств и указанием реквизитов лица, их получившего. Также необходимо зафиксировать все взаимодействия   
с преступниками – адрес сайта и электронной почты, номер телефона, физический адрес офиса злоумышленников и т. д. При этом в случаях, где мошенничество связано с хищением денежных средств или конфиденциальной банковской информации, самым первым шагом должен быть звонок обслуживающему банку и блокировка карт. Чем раньше банк будет уведомлен о произошедшем неправомерном списании денежных средств, тем больше шансов, что он сможет оказать содействие клиенту на дальнейших этапах.

Будьте бдительны, не сообщайте третьим лицам свои персональные данные и данные банковских карт.

Межрайонный прокурор М.А. Калгин