****

**Информация**

**по вопросам профилактики преступности в сфере iT - технологий**

На сегодняшний день можно выделить несколько наиболее распространённых способов дистанционных хищений:

***1***.***Звонок от имени сотрудника правоохранительных органов либо от родственника, который находится в полиции и дальнейшее пояснение о том, что близкий человек совершил преступление или ДТП со смертельным исходом и необходима крупная сумма денежных средств, чтобы избежать ответственности.***

***2.Звонок от имени сотрудника банка или сотрудника правоохранительных органов, пояснение о том, что с Вашей банковской карты происходит попытка списания денежных средств, либо на Ваше имя пытаются оформить кредит злоумышленники.***

***3.Инвестирование денежных средств на различных платформах в крупные и известные финансовые корпорации, например, такие как «Газпром», «Тинькофф» и другие.***

***4.Перевод предоплаты за приобретение товара в сети Интернет на различных площадках.***

***5.Продажа товара в сети Интернет и переход по присылаемой «ссылке» для получения денежных средств заранее, на банковскую карту.***

***6.Поступление сообщения от родственников или знакомых в социальных сетях с просьбой занять денежные средства.***

**Помимо изложенного, есть еще ряд простых общих рекомендаций**:

1. Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Установите и обязательно обновляйте антивирусные программы.

2. Проверяйте информацию о состоянии счетов, зачислении или списании денежных средств с них, в достоверных источниках, закажите выписку в банке, получите консультацию специалиста банка.

3. Никому не сообщайте персональные данные, в том числе пароли и коды доступа. Не храните данные карт на компьютере и в смартфоне.