**Информация по предупреждению преступлений, связанных с хищением денежных средств граждан с использованием современных информационно-телекоммуникационных технологий**

На территории Семилукского района Воронежской области актуальной остаётся проблема хищения денежных средств граждан с использованием современных информационно-телекоммуникационных технологий. Так, за 2023 год на территории района зарегистрировано 144 преступления данной категории, ущерб по которым составил свыше 20 млн рублей. Потерпевшими становятся жители различных возрастных групп. Преступники при совершении хищений постоянно совершенствуются, придумывая новые способы, при этом активно используют Интернет-ресурсы, торговые площадки, возможности цифровой телефонии.

На сегодняшний день наиболее часто встречаются следующие способы совершения дистанционных хищений:

1. *Звонок сотрудника банка* – когда неизвестное лицо представляется сотрудником службы безопасности какого-либо банка и сообщает, что с Вашего банковского счета происходят операции по несанкционированному списанию денежных средств, и в целях безопасности счета предлагает перевести сбережения на «резервный» или «безопасный» счет. Распространены случае сообщения информации об оформлении на Вас кредита и необходимости пройти в приложении онлайн-Банка по определённой ссылке для его аннулирования (выполнить иные инструкции).

2. *Звонок сотрудника правоохранительных органов* – неизвестное лицо представляется сотрудником правоохранительных органов и сообщает, что проводится спецоперация по поимке мошенников и для этого необходимо перевести деньги на «специальный» счет. При этом требует не звонить в банк, так как сотрудники банка заодно с мошенниками.

3. *Телефонный звонок от близкого друга или родственника* с просьбой о помощи: требование/просьба перевести определенную сумму, в связи с тем, что близкий родственник либо знакомый находится в опасности, либо задержан сотрудниками правоохранительных органов. В данном случае преступники предлагают решить вопрос, для чего требуется определенная сумма денег, которую в последующем забирают через таксистов, либо предлагают зачислить денежные средства на банковские реквизиты.

4. *Обман при покупке (продаже) товара на интернет-сайтах*. Предоплата за несуществующий товар – подается объявление на востребованный товар с привлекательной ценой (ниже рыночной) с приложением ненастоящих фотографий.

5. *Ошибочный перевод средств на банковский счет* с просьбой вернуть деньги.

Как обезопасить себя от мошенников:

1. *Проверять информацию*, полученную в ходе телефонного разговора и интернет переписки с неизвестными (они могут представляться сотрудниками правоохранительных органов, представителями кредитных организаций).
2. *Установить на телефон* (компьютер) современное лицензированное антивирусное программное обеспечение.
3. *Не устанавливать и не сохранять файлы*, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте.
4. *Используйте сложные пароли*, не связанные с Вашими персональными данными (имя, день рождения, место жительства).
5. Ни при каких обстоятельствах *не сообщать реквизиты своих банковских счетов (карт), пароли и другую персональную информацию*.
6. *Поставить лимит на сумму списаний или перевода* в личном кабинете банка.
7. *По всем возникающим вопросам обращаться в банк*, выдавший карту.
8. *Не выполнять никаких срочных запросов к действию*, в том числе по установке каких бы то ни было приложений.
9. *Не переходить по ссылкам*, которые приходят на e-mail или по SMS.
10. *Обращать на все сообщения* от банка (например, если они содержат грамматические ошибки).
11. *Не перезванивать по незнакомым номерам*, которые приходят на e-mail или по SMS.
12. *Перепроверять подлинность интернет-сайтов*, на которых осуществляете заказ товара.