Несмотря на все принимаемые меры, продолжает существовать тенденция к росту числа преступлений, связанных с кражами денежных средств с банковских счетов граждан, в связи с чем проблема остается актуальной.

## Распространенные способы мошенничества:

* Мошенники представляясь банковскими сотрудниками («службой безопасности» или «службой финансового мониторинга»), сообщают о подозрительной активности и **предлагают продиктовать данные карты**, чтобы банк принял меры по защите средств.
* Убеждают **перевести деньги на отдельный счет** якобы для их защиты, предложив сделать это онлайн либо сняв деньги в банкомате.
* Просят **установить специальное программное обеспечение для «защиты средств»**, с помощью которого мошенники могут узнать данные карты, после чего вывести средства.
* С начала пандемии мошенники активно **эксплуатируют тему коронавируса**, будь то «бесплатная» диагностика, медицинская помощь, пособия, компенсации и другие предлоги, конечной целью которых является перевод денег.
* **Сообщают пожилым людям о положенных выплатах** от имени сотрудников Пенсионного фонда, в этом случае узнать номер банковской карты и другие данные им нужноякобы для перечисления денег.

## Еще одним видом мошенничества является почтовый фишинг, мошенничество посредствам соцсетей и поддельных сайтов

* Рассылаемые мошенниками письма могут содержать ссылки на поддельные **сайты, имитирующие странички интернет-магазинов** с большими скидками, а также отелей, сервисов по продаже авиабилетов, страховых компаний, различных ведомств. Письма приходят также под видом квитанций об оплате коммунальных платежей или в виде официальных уведомлений от банков и других организаций.
* Еще один популярный способ мошенничества связан с **продажами на сайтах объявлений**, где покупатель по поддельной ссылке вводит данные для оплаты несуществующего товара либо перечисляет часть денежных средств за «бронирование» товара.
* В соцсетях мошенники делают **рассылки по списку друзей** **со взломанного аккаунта** с просьбой перевести денег на карту. Подобную информацию всегда необходимо перепроверять по другим каналам связи.

**В целях исключения мошеннических действий** не стоит сообщать третьим лицам данные карты, в том числе четырехзначный PIN-код и трехзначный CVC-код, указанный на обороте карты. Стоит учесть, что при звонках от мошенников могут отображаться реальные номера банковских телефонов. Они могут представляться также полицейскими или работниками бюро кредитных историй.

**Важно!** Не нужно переходить по ссылкам из подозрительных писем и загружать неизвестные программы. Остерегайтесь оплачивать покупки на подозрительных сайтах, не переводите деньги, если нет уверенности в получателе. Контролируйте все операции по счету и пользуйтесь антивирусными программами.