

- не сообщайте персональные данные, а также информацию о банковских картах и счетах (номера, коды доступа, пароли);
- не берите по инициативе третьих лиц кредиты на свое имя;
- не переводите свои либо кредитные денежные средства на счета продиктованные мошенниками, представляющих сотрудниками банков, правоохранительных органов, операторов связи.

ВНИМАНИЕ!

Остерегайтесь мошенников, которые любыми способами пытаются завладеть персональными данными, денежными средствами.

Будьте бдительны!

О фактах мошенничества сообщайте в правоохранительные органы Новониколаевского района



**Прокуратура
Новониколаевского
района**



**Дистанционное
мошенничество**

2024 г.

Способы совершения преступлений:

- звонок от лица службы безопасности банка и совершение хищения денежных средств под предлогом предотвращения их «списания» с банковского счета гражданина;
- звонок от лица службы безопасности банка с целью оформления встречного кредита и предотвращения мошеннических действий по счетам;
- звонок от лица представителей сотовых операторов под предлогом продления договора пользования услугами операторов связи;
- звонок от лица сотрудников правоохранительных органов в связи с необходимостью получения сведений для доступа в системы удаленного банковского обслуживания;

- оформление онлайн-кредитов, при установке гражданами программ удаленного доступа к своим электронным устройствам и передаче прав управления ими третьим лицам (к примеру, RustDesk);
- смс сообщения посредством мессенджеров, социальных сетей о просьбе занять в долг, в том числе и с аккаунтов, профилей знакомых лиц, так как их страница может быть взломана мошенниками.

Противодействие:

- игнорировать сообщения о предоставлении личной информации;
- сотрудники банков, правоохранительных органов, сотовых операторов не используют в профессиональной деятельности мессенджеры Telegram, WhatsApp;

- в случае поступления звонков от сотрудников банков, правоохранительных органов, сотовых операторов не сообщать персональные данные, коды подтверждений, приходящих по смс;
- при использовании сайтов бесплатных объявлений проверяйте порядочность продавца на сайтах Юла, Avito;
- при поступлении заманчивых предложений получения займов/кредитов обращайтесь в офисы банков либо используйте официальные сайты банков;
- обращайте внимание на гиперссылку сайта, так как фальшивые письма и сайты могут повторять дизайн настоящих, однако гиперссылки будут с ошибками, к примеру сайт Промсвязьбанка :<https://www.psbank.ru>, а сайт мошенников (фишинговый) <https://www.2psbank.ru>;