| ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИПрокуратура Смоленской области **Прокуратура Новодугинского района** |
| --- |

Прокуратура Новодугинского района информирует Вас о том, что в настоящее время широкое распространение получили случаи телефонного и интернет-мошенничества, а также кражи денежных средств с банковских карт.

**В связи с этим просим Вас проявлять бдительность и не передавать сведения своих банковских карт не знакомым лицам, а также не переводить денежные средства на чей-либо счет.**

В настоящее время в России злоумышленниками стали широко применяться различные приложения и платформы (например, такие как RustDesk), а также социальные сети (Telegram, WhatsApp, Viber и др.), с помощью которых, введя в заблуждение наивных граждан, легко присвоить денежные средства, принадлежащие Вам и Вашим близким.

Так,мошенники звонят клиентам банков по фрагментам базы, «утекшим» из Сбербанка, ВТБ, Тинькофф и другим, применяют приемы «социальной инженерии».

Телефонные мошенники говорят, что они «из банка», «из правоохранительных органов системы ФСБ, МВД, Следственного комитета, Прокуратуры», разными приемами запугивают будущую жертву и принуждают поставить на свой смартфон различные программы, которые якобы помогут воспрепятствовать краже денег, мошенническому переводу, взятию кредита и т.п.; либо просто взять кредит и перевести на какой-либо счет деньги. При этом часто мошенники в социальных сетях присылают скриншоты «поддельных» служебных документов, таких как копии служебных удостоверений, банковский уведомлений, копии постановлений о возбуждении уголовного дела и т.п.

ЗАПОМНИТЕ! Сотрудники правоохранительных служб не имеют право направлять физическим лицам копии служебных документов посредством социальных сетей, а также не уполномочены просить физических лиц осуществлять какие-либо действия, связанные со сведениями, составляющими банковскую тайну, в том числе предоставить личные данные по телефону или посредством социальных сетей, например, ФИО, дата рождения, номер счета и иные сведения.

Кроме того, такие действия по телефону или посредством социальных сетей не могут выяснять или просить предоставить и сотрудники банковских организаций.

При этом, мошенники могут назвать установленную программу «поддержка Сбербанка», «поддержка ВТБ», просто «поддержка», антивирус или как-то еще.

Разъясняем, что после установки программ и платформ или перехода по сторонним ссылкам, жертва передает мошенникам свои персональные данные, даёт согласие на подключение, и мошенники получают полный доступ к смартфону через интернет. Дальше они могут делать что угодно, в том числе вывести все деньги потерпевшего в другой банк.

**ДОКАЗАТЬ ВЗЛОМ СЧЕТА В ДАННОМ СЛУЧАЕ БУДЕТ НЕВОЗМОЖНО**, т.к. взаимодействовать с банком в данном случае будет непосредственно Ваш телефон или компьютер и всю ответственность в таком случае за перевод СВОИХ денежных средств постороннему лицу несёте именно ВЫ.

**ЧТО НУЖНО ДЕЛАТЬ, ЧТОБЫ УБЕРЕЧЬ СЕБЯ ОТ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ МОШЕННИКА:**

1. Никогда не ставить в свой телефон каких-либо программ, устанавливать платформы и переходить по сторонним ссылкам ПО ЧЬЕЙ-ЛИБО ПРОСЬБЕ.
2. Ни в коем случае никому и никогда не сообщать свои персональные, банковские данные (в том числе ФИО, дату рождения, адрес проживания и регистрации, сведения о серии и номере паспорта, а также о дате и органе его выдававшем, пароли и логины от электронных почтовых ящиков, пароли и пин-коды от банковских карт, страховые и медицинские сведения, а также пароли для входа в онлайн приложения банков).
3. Внимательно читать текст всех СМС и Push-сообщений. В случае наличия ссылки для перехода на какой-либо сторонний сайт НЕ ПЕРЕХОДИТЬ ПО НИМ.
4. Не сообщать коды из СМС-сообщений «сотрудникам банка», «правоохранительным органам», «роботу» или иным лицам по телефону или посредством социальных сетей.
5. Не разговаривать с людьми, представляющимися работниками банков, либо правоохранительных органов, которые хотят узнать у Вас любые данные. В случае просьбы предоставления Ваших данных по телефону или социальным сетям – ПРЕКРАЩАТЬ РАЗГОВОР.
6. В случае возникновения каких-либо сомнений о наличии кредитов, каких-либо несанкционированных списаний и т.п. – ЛИЧНО обращаться в свой банк.