

**БУДЬТЕ ВНИМАТЕЛЬНЫ!**

Прокуратура Зареченского района г.Тулы разъясняет, чтобы обезопасить себя от действий мошенников, необходимо придерживаться следующих рекомендаций:

-не сообщать конфиденциальные данные карты третьим лицам (срок, CVV-код и ПИН-код);

-подключить услугу СМС-уведомлений для контроля за счётом;

-ПИН-код хранить отдельно от карточки и прикрывать рукой клавиатуру банкомата или терминала в момент его ввода;

-установить расходные лимиты в интернет-банке или мобильном приложении;

-никогда никому не сообщать код из СМС для подтверждения операции, которую клиент не совершал (сотрудники банка не вправе запрашивать данную информацию);

-немедленно блокировать карту в случае утраты, кражи или захвата её банкоматом, а также при утере телефона с привязанным номером.

**Если у Вас списали деньги, вы получили СМС-уведомление, немедленно заблокируйте карту и обратитесь в банк с отказом от последней транзакции. Затем попросите отчет с указанием номера счета получателя, затем напишите заявление в полицию, сотрудники правоохранительных органов должны возбудить уголовное дело по факту мошенничества.**

**Правила безопасности при пользовании дистанционного банковского обслуживания (банкинга)**

Чтобы пользоваться банкингом без риска утраты денег, необходимо соблюдать следующие базовые меры предосторожности.

* Не входите в интернет-банк с чужих компьютеров или из публичных незащищенных сетей. Если же это всё-таки случилось, по завершении сессии нажмите «Выход» и очистите кэш.
* На личном компьютере установите антивирус и своевременно его обновляйте. Используйте современные версии браузера и почтовых программ.
* Не скачивайте файлы, полученные из непроверенных источников, не переходите по ненадёжным ссылкам. Не открывайте подозрительные письма и сразу же блокируйте их отправителя.
* Без необходимости не вводите никакие свои персональные данные, помимо логина и пароля.
* Проверяйте адресную строку. Должно использоваться защищённое HTTPS-соединение. А малейшее несовпадение с доменом банка почти наверняка означает, что вы находитесь на фишинговом сайте.
* Придумайте сложный пароль для входа в личный кабинет, а также используйте одноразовые пароли, запрашиваемые банками для подтверждения действий в личном кабинете.

*Обратите внимание! Банки не рассылают сообщений о блокировке карт, а в телефонном разговоре не пытаются установить конфиденциальные сведения и коды, связанные с картами клиентов.*

Проинформируйте банк, если сменили номер или потеряли SIM-карту. Установите пароль на телефон и не снимайте блок с экрана, если кто-то посторонний наблюдает за вашими действиями. А если SIM-карта оформлена на вас лично, то запретите её замену по доверенности.