



Всем главам муниципальных образований
Ташлинского района
Оренбургской области

ПРОКУРАТУРА
Российской Федерации
ПРОКУРАТУРА
ТАШЛИНСКОГО РАЙОНА
ОРЕНБУРГСКОЙ ОБЛАСТИ

ул. Хлебная, 10а, с. Ташла, 461170
тел. (35347) 2-23-57 факс: (35347) 2-12-76

20.04.2021 № 40-1-2021
на № _____

В целях профилактики мошеннических действий, в том числе с использованием электронных средств платежа (банковские карты, телефоны и т.д.), направляется разработанная прокуратурой Ташлинского района памятка «О мерах по предупреждению хищения денежных средств при использовании банковских карт».

Прошу распространить памятку среди органов и организаций, расположенных в муниципальном образовании, а также среди населения, в том числе разместить памятку на информационных стендах.

Приложение: памятка.

Заместитель прокурора района

советник юстиции

Н.С. Ефимов

Наиболее распространенные схемы телефонного мошенничества:

Тактика телефонных

мошенников.

Общая информация о потенциальной

телефонной мошенничестве

IS, либо телефонный звонок.

SMS – это мошенничество

«звонящий»: такие сообщения

посылаются в большом объеме –

в надежде на доверчивого

участника. Телефонный звонок

позволяет манипулировать

мошенником при разговоре, но при

общении можно разоблачить

мошенника правильным вопросом.

Мошенники – заставить Вас

передать свои денежные средства

«добровольно». Для этого

используются различные схемы

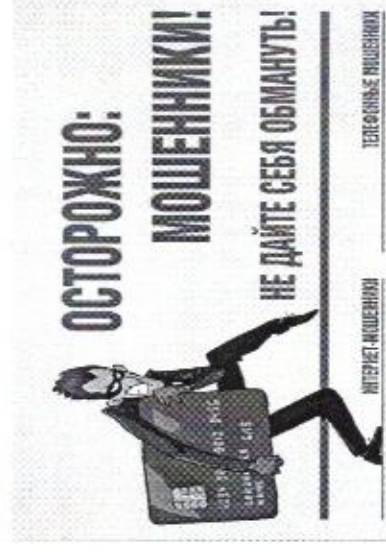
мошенничества.



Прокуратура Ташлинского района Оренбургской области

ПАМЯТКА

О мерах по предупреждению
хищений денежных средств при
использовании банковских карт
2021 г.



В случае, если Вы стали жертвами
мошеннических действий, в том числе при
попытках каких-либо лиц неправомерно
завладеть Вашими денежными средствами с
использованием банковских карт, необходимо
обращаться в ОМВД России по Ташлинскому
району по адресу: Оренбургская область,
Ташлинский район, с.Ташла ул.Хлебная, д.15,
тел. 8(35347)2-10-86
или в прокуратуру Ташлинского района по
адресу: Оренбургская область, Ташлинский
район, с.Ташла ул.Хлебная, д.10а, тел.
8(35347)2-12-76

Владельцам пластиковых банковских карт

рекомендуется!

Никогда и никому не сообщайте ПИН-код Вашей карты.

Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами.

Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

Ваша карта – только Ваша!

Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелек, не пересчитывая сумму в нём.

Ни у кого нет права требовать Ваш ПИН-код

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите ее выполнять. Позвоните в указанную организацию и сообщите о данном факте.

Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

Помните! хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

Немедленно блокируйте карту при ее утере

Пользуйтесь защищенными банкоматами

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраны.

Опасайтесь посторонних

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Набирая ПИН-код, прикрывайте клавиатуру рукой.

Банкомат должен быть «чистым» от посторонних устройств и полностью исправен

Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком – он обязан предоставить консультационные услуги по работе с картой.

Не доверяйте карту официантам и продавцам

Банк может инициировать общение с клиентом только для консультаций по продуктам и услугам кредитно-финансового учреждения. При этом звонки совершаются с номеров, указанных на оборотной стороне карты, на сайте банка или в оригинальных банковских документах. Иные номера не имеют никакого отношения к банку.

Следует использовать только надежные официальные каналы связи с кредитно-финансовым учреждением. В частности, форму обратной связи на сайте банка, онлайн-приложения, телефоны горячей линии, группы или чат-боты в мессенджерах (если таковые имеются), а также официальные банковские приложения из магазинов App Store, Google Play, Microsoft Store.

Необходимо учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать:

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону (факсу);
- сообщения кодов третьим лицам (в противном случае любые операции, совершенные с использованием ПИН-кода или CVV-кода, считаются выполненными самим держателем карты и не могут быть оспорены).

При использовании банкоматов отдавайте предпочтение тем, которые установлены в защищенных местах (например, в госучреждениях, офисах банков, крупных торговых центрах).

и предотвращения противоправных действий по снятию денежных средств с банковского счета необходимо исходить следующего.

руководки банка никогда по телефону в электронном письме **не разглашают:**

персональные сведения (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);

реквизиты и срок действия карты;

ароматы или коды из СМС-сообщений подтверждающих финансовых операций и их отмены;

логи, ПИН-код и CVV-код банковских карт.

руководки банка также **не предлагают:**

установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);

перейти по ссылке из СМС-сообщения; включить переадресацию на телефоне клиента для совершения в дальнейшем банка от его имени в банк;

под их руководством перевести для хранения денежные средства на защищенный счет;

йти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.