Тактика телефонных мошенников.

ия общения с потенциальной
ртвой мошенники используют
IS, либо телефонный звонок.
SMS – это мошенничество
зслепую»: такие сообщения
сылаются в большом объеме –
в надежде на доверчивого
учателя. Телефонный звонок
позволяет манипулировать
овеком при разговоре, но при
м общении можно разоблачить
енника правильным вопросом.
ь мошенников – заставить Вас
здать свои денежные средства
«добровольно». Для этого
ользуются различные схемы
мошенничества.

Наиболее распространенные схемы телефонного мошенничества:

«ВАША КАРТА ЗАБЛОКИРОВАНА» SMS-сообщение о якобы заблокированной банковской карте, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата.

«РОДСТВЕННИК В БЕДЕ» Требование крупной суммы денег для решения проблемы с якобы попавшим в беду родственником.

«ВЫ ВЫИГРАЛИ» SMS-сообщение о том, что вы стали победителем и вам положен приз.

«ВИРУСНАЯ АТАКА» SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащий вредоносную программу, дающую доступ мошенникам к вашей банковской карте.

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ» Вам якобы положена компенсация за приобретаемые ранее товары, для получения которой вам необходимо оплатить какие-либо пошлины или проценты.

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ» Вас просят вернуть деньги за ошибочный перевод, дополнительно снимая средства со счета по чеку.

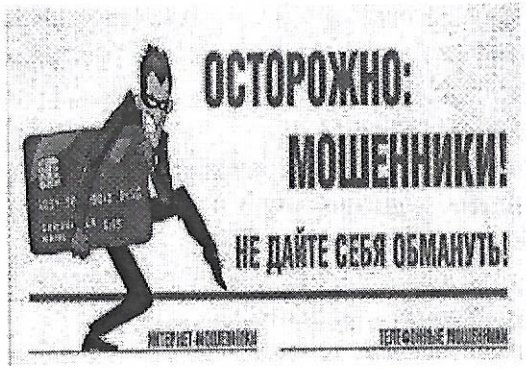
В случае, если Вы стали жертвами мошеннических действий, в том числе при попытках каких-либо лиц неправомерно завладеть Вашими денежными средствами с использованием банковских карт, необходимо обращаться в ОМВД России по Ташлинскому району по адресу: Оренбургская область, Ташлинский район, с.Ташла ул.Хлебная, 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

Прокуратура Ташлинского района Оренбургской области

ПАМЯТКА

О мерах по предупреждению хищений денежных средств при использовании банковских карт

2021 г.



и предотвращения противоправных
ствий по снятию денежных средств с
ковского счета необходимо исходить
ледующего.
рудники банка никогда по телефону
в электронном письме **не**
рашивают:
ерсональные сведения (серия и номер
порта, адрес регистрации, имя и
илия владельца карты);
квизиты и срок действия карты;
ароли или коды из СМС-сообщений
подтверждения финансовых операций
их отмены;
огин, ПИН-код и CVV-код банковских
т.
рудники банка также **не предлагают**:
установить программы удаленного
ступа (или сторонние приложения) на
бильное устройство и разрешить
ключение к ним под предлогом
нической поддержки (например,
ление вирусов с устройства);
ерейти по ссылке из СМС-сообщения;
ключить переадресацию на телефоне
иента для совершения в дальнейшем
нка от его имени в банк;
под их руководством перевести для
хранности денежные средства на
щищенный счет»;
йти в онлайн-кабинет по ссылке из
С-сообщения или электронного письма.

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 опротестованы).

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

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 счет, заблокировав карту после кражи или утери.

Ваша карта – только Ваша!

Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, 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 охраной.

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