|  |  |
| --- | --- |
| Наиболее частыми видами и способами мошенничества являются:  | Как не стать жертвой мошенников при использовании банковской карты и совершении электронных платежей?  |
| * предоплата или полная оплата товара на интернетсайте частных объявлений либо в социальных сетях за товар, который не видели вживую. После перевода денежных средств, продавец, зачастую, перестаёт выходить на связь;
* предоплата или полная оплата брендового товара на интернет-сайте, являющимся подделкой сайта официального производителя, для последующей доставки по почте. Такие мошенники, получив деньги, исчезают вместе с интернет-сайтом в течение нескольких месяцев работы;
* поступление СМС-сообщения с указанием контактного телефонного номера либо звонка якобы от сотрудника банка с информацией о блокировке карты либо о совершении подозрительных операций с банковским счётом. Фактически звонок осуществляется мошенником, который спросит номер карты, CVC-код, а также иные идентифицирующие Вас данные. В дальнейшем, использовав эту информацию, злоумышленник переведёт деньги на свой счёт;
* от незнакомого абонента приходит сообщение о зачислении на ваш мобильный телефон платежа. В дальнейшем, как правило, с этого же номера поступает просьба вернуть ошибочно оплаченные деньги;
* оплата процентов, налогов или доставки предлагаемых несуществующих крупных выигрышей и выгодных кредитов. Такой вид мошенничества, как правило, характерен для социальных сетей;
* звонок от близкого человека с просьбой помочь финансово в целях избежание внезапно возникших проблем (дать взятку сотруднику ГИБДД за сбитого пешехода, оплатить срочную операцию);
* скимминг, то есть считывание при помощи специального устройства данных с магнитной полосы карты.

  | * Запишите в телефонную книгу контактные номера родных, близких и коллег, а также телефоны горячих линий банка, чтобы идентифицировать того, кто Вам звонит.
* При звонке с незнакомого номера от имени родственника с просьбой срочно перевести деньги под любым предлогом прервите разговор. Перезвоните тому, от чьего имени обращался звонивший, чтобы узнать, действительно ли ему нужна помощь.
* Если сомневаетесь, что вам позвонил сотрудник банка, попросите его перезвонить через несколько минут. Банковский служащий обязательно совершит повторный звонок, а Вы за это время успеете обратиться на горячую линию банка и узнать, не мошенник ли Вам звонил.
* Не реагируйте на СМС-сообщения с незнакомых номеров.
* Не передавайте Вашу банковскую карту и пароль от нее посторонним лицам.
* Не сообщайте посторонним лицам ваши паспортные данные, реквизиты банковской карты, данные для входа в интернет-банк, а также СМС-сообщения с кодом подтверждения проведения банковских операций.
* Не используйте один пароль для всех Интернет- ресурсов.
* Не совершайте покупки на сайтах, не внушающих доверия.
* Не держите на карте, предназначенной для интернет- покупок, большие суммы.

  | * Если к Вам поступила информация о победе в розыгрыше, выйдете на связь с его организаторами. Постарайтесь получить от них максимально возможную информацию об акции: условиях участия в ней и правилах ее проведения. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов. Помните, что упоминание вашего имени на Интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией вашего выигрыша. Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас.
* При смене номера телефона, к которому подключен мобильный банк, обратитесь в отделение банка с заявлением о прекращении предоставлении услуги по старому номеру телефона.
* При использовании банкомата обратите внимание, исправен ли он, размещена ли информация о владельце банкомата, крепко ли прикреплена клавиатура, а также устройство приёма карт. Некоторые мошенники используют специальных технические приспособления, прикрепляющиеся на банкоматы и позволяющие считать магнитную ленту банковской карты и узнать пин-код.
* Не просите о помощи посторонних в случае возникновения сложностей при снятии денег в банкомате, обратитесь непосредственно к сотрудникам банка. - Не используйте Вашу банковскую карту, с возможностью безконтактной оплаты, на виду у посторонних лиц.
* При утрате банковской карты незамедлительно обратитесь в кредитную организацию (банк), либо на горячую линию банка в целях ее блокировки.
 |

ПРОКУРАТУРА АСТРАХАНСКОЙ ОБЛАСТИ

Прокуратура Приволжского района



Мошенничество при использовании

 банковской карты и совершении

электронных платежей

2022 год

с.Началово