СИМ - КАРТЫ

Новые уловки мошенников по мобильным телефонам направлены на получение сведений о паспорте абонента. Эта информация относится к категории персональных данных и защищена законом, однако он не может помешать абоненту выдать их злоумышленнику по доброй воле.

Если вам звонит оператор с предложением пролонгации номера или любым другим, самое простое и очевидное, что вы можете сделать – прервать разговор, сославшись на то, что сейчас вам неудобно его вести.

Не исключено, что обращение кажется вам актуальным. Помните, что большинство вопросов легко решить через личный кабинет в приложении оператора мобильной связи. Менее удобный, но более надежный способ – посетить ближайший салон вашего провайдера, сообщить о входящих звонках и продлить симку, если это нужно.

Мошенники – «сотовые операторы» действуют по такому алгоритму:

- Абонент принимает звонок от сотрудника одной из компаний, предоставляющих мобильную связь.

- Звонящий информирует об окончании срока действия сим-карты. Другой вариант – завершение срока действия договора на обслуживание.

- На вопрос абонента, почему у него не отображается информация об этом в личном кабинете, аферист говорит, что это невозможно по ряду причин, поэтому происходит устное информирование.

- Звонок от мошенника продолжается: теперь клиента просят сообщить личные данные или продиктовать SMS, открывающее доступ к личному кабинету. Другим предметом интереса преступников является вход в аккаунт пользователя на Госуслугах – для этого также требуется номер телефона и уникальный код, который может сообщить только его владелец.

Принципиальная разница в поведении аферистов и представителей сотовой компании – отношение к абоненту.

Первые невероятно напористы, торопят, пытаются захватить собеседника врасплох. Вторые с пониманием относятся к тому, что человек может быть занят, готовы ждать более подходящего момента для разговора или использовать другие способы донесения информации (например, не звонком, а с помощью уведомления в личном кабинете).

Достаточно простая проверка – это сказать, что вам нужно отойти от телефона. Его необходимо в буквальном смысле положить на стол и сделать шаг в сторону. Представитель сотовой компании предложит перезвонить или подождет, а преступник будет давить и пугать необратимыми последствиями.

Точно указывает на нечистоплотность звонящего:

- предложение назвать код доступа для входа в личный кабинет или в аккаунт на Госуслугах;

-утверждение, что договор будет расторгнут в течение 24 часов в одностороннем порядке;

- указание перевести деньги по любой из возможных причин (в качестве абонентской платы, для приостановки расторжения договора, на защищенный счет в Центробанке и т.д.).

Телефонные мошенники придумали новую легенду для своих жертв: якобы подтверждение личных данных возможно только через Госуслуги, войти туда нужно немедленно, непосредственно в процессе диалога по телефону.

Если вы попытались открыть свой аккаунт на портале, увидели, что он заблокирован, не спешите предпринимать какие-либо действия. Разблокировка происходит с помощью контрольного вопроса, ответ на который знаете только вы! А мошенники будут пытаться проникнуть в ваш кабинет на Госуслугах, используя коды доступа, которые сами же и отправят на ваш смартфон.

Одним словом, если что-то идет явно не так, если вас настораживает и диалог в частности, и ситуация вообще, немедленно прервите разговор и не отвечайте на входящие с неизвестных номеров.

ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.

СООБЩЕНИЯ ОТ ДРУЗЕЙ

Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель – узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫИГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».

ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не проходите по сомнительным ссылкам.