**Алло, это аферисты? Что отвечать мошенникам, чтобы они больше не звонили**

Более четверти владельцев банковских карт в зоне риска стать жертвой аферистов – они могут назвать мошенникам персональные данные своих карточек (срок действия и CVC-код), говорится в материалах аналитического центра Национального агентства финансовых исследований (НАФИ).

Оказывается, лишь 10% наших соотечественников знают, какие данные карты можно сообщать сотруднику банку: ее номер, фамилию и имя держателя.

С мошенниками сталкивались 31% россиян, чаще всего злоумышленники звонили им по телефону и пытались вытянуть персональную информацию с помощью социальной инженерии. Как аферисты крадут деньги и что отвечать, когда звонят из «службы безопасности» банка.

**Миллионные манипуляции**

Самая популярная (и самая действенная) мошенническая схема выглядит следующим образом: гражданину звонят из банка и сообщают, что с его счета была совершена сомнительная операция, например перевод кругленькой суммы в другой регион или даже в другую страну.

Злоумышленники активно применяют методы социальной инженерии: на них приходится почти две трети всех хищений с банковских счетов россиян, свидетельствуют данные Центрального банка РФ. Аферисты заранее собираются необходимую информацию о потенциальной жертве, с постоянными утечками персональных данных граждан это не так сложно. Часть мошенники звонят своим жертвам рано утром или, наоборот, в разгар рабочего дня, чтобы застать человека врасплох, не дать ему возможности как следует обдумать происходящее.

«Уверенный и спокойный мужской голос обращается к вам по имени и отчеству, чтобы вызвать доверие, представляется сотрудником службы безопасности банка и действует по одному из основных сценариев:

* сообщает о подозрительной активности с вашей банковской картой. Например, о попытке перевести крупную сумму или о запросе на банковскую операцию из другого региона, где вы никогда не были. В целях отмены несанкционированной операции просит назвать полный номер вашей банковской карты и код подтверждения из смс, поступившем от банка. Аферист сам предупреждает вас, что смс-код никому нельзя сообщать и просит ввести его в тоновом режиме, чем усыпляет вашу бдительность;
* сообщает о попытке несанкционированного списания денежных средств с вашего счета и предлагает перевести деньги на „безопасный счет“, который, естественно, принадлежит мошенникам. Если вы не соглашаетесь, может пригрозить штрафом за отказ перевода денежных средств;
* сообщает о выявлении вредоносного программного обеспечения на вашем смартфоне. Для устранения просит предоставить доступ к устройству, установив на гаджет программу удаленного доступа TeamViewer или Anydesk. Вы устанавливаете программу и обеспечиваете непосредственный доступ злоумышленников к вашему банковскому счету», – перечисляет **эксперт Национального центра финансовой грамотности, консультант по финансовой грамотности проекта вашифинансы.рф Наталья Шумакова**.

Граждане верят в эти нехитрые манипуляции и остаются без денег. Вот, например, история из Белгорода, где пенсионерка перевела аферистам ... 3,5 миллиона рублей. Женщине позвонили якобы из банка и сообщили, что кто-то пытался снять с ее счета 4,5 тысячи рублей, когда растерявшаяся белгородка ответила, что это не она, ее перевели на сотрудника «службы безопасности», а потом даже на сотрудника «полиции». Собеседники убедили пенсионерку, что помогут спасти ее деньги.

«Женщину предупредили, что она должна зарядить телефон, постоянно быть на связи и четко следовать всем инструкциям. Выполняя указания незнакомцев, женщина сняла хранившиеся в нескольких банках денежные средства и частями через разные банкоматы перевела более 3 500 000 рублей на счета злоумышленников», – говорится в сообщении пресс-службы УМВД России по Белгородской области.

**Как общаться с аферистами?**

Определить, что вам звонит мошенник, на самом деле очень просто: настоящий банковский служащий никогда не спросит срок действия карты, CVC-код, логин и пароль от мобильного банка, одноразовый пароль из смс-сообщения, не предложит перевести деньги на некий резервный счет.

Поэтому первое правило, когда вам позвонили и сказали о сомнительном переводе с вашего счета, – не называть собеседнику персональную информацию. «Никому не сообщайте персональные данные (паспорт, СНИЛС) или данные банковской карты (номер, срок действия, ПИН-код, смс-код безопасности). Даже если вас просит об этом сотрудник или служба безопасности банка. Банк обладает всей необходимой для совершения операций информацией, а сотрудники банка не имеют права запрашивать ее у вас», – напоминает Шумакова.

Да, не теряйте бдительность, если вам позвонили с реального телефона банка, того, что указан на карте или на официальном сайте финансового учреждения. Мошенники могут имитировать звонок с любого телефона – в интернете полно сайтов, предлагающих услугу подмены номера.

Не соглашайтесь переводить деньги со своего банковского счета или своей банковской карты на «безопасный счет» из-за сбоя или угрозы мошенничества. Запомните: самый безопасный счет для ваших денег – это ваш счет, говорит Шумакова.

Требований назвать персональную информацию и предложений перевести деньги на резервный счет достаточно для того, чтобы понять, что вы имеете дело с мошенниками. «Чувствуете, что разговор подозрительный или нестандартный, даже если звонок с настоящего номера банка, положите трубку и сами перезвоните по номеру телефона, указанному на обратной стороне карты», – советует Шумакова.

Как вариант, над аферистами можно пошутить. Обычно мошенников ставит в тупик, когда их потенциальные жертвы признаются, что да, переводили 100 тысяч рублей в Сыктывкар. А на просьбу назвать срок действия карты, CVC-код, логин и пароль от мобильного банка можно продиктовать выдуманные данные. Злоумышленники убедятся, что вас не обмануть, и, скорее всего, больше вас беспокоить не будут.

***А.В. Мартынов, заместитель начальника отдела – начальник полиции МО МВД России по ЗАТО п. Сибирский майор полиции***