Прокуратура Нагорского района проведёт «горячую линию» по вопросам финансовой грамотности населения

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.

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 собирают необходимую информацию о потенциальной жертве, с постоянными утечками персональных данных граждан это не так сложно. Часто 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».

Граждане верят в эти нехитрые манипуляции и остаются без денег.

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».

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.

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 — советуют специалисты.

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.

Важно помнить!

- Никому не сообщайте пин-код вашей карты, ваши пароли. Храните карту и пин-код раздельно. Придумывайте сложные пароли, не используйте простые комбинации цифр, свою фамилию, даты рождения, имена детей и т.п. Используйте разные пароли для входа на разные интернет-ресурсы.
- Никому не позволяйте пользоваться вашей пластиковой картой.
- При вводе пин-кода прикрывайте клавиатуру, чтобы с камеры не была видна комбинация цифр пин-кода.

- Для оплаты покупок через Интернет заведите отдельную виртуальную карту и установите суточные лимиты для совершения покупок. Установите на банковских картах лимит выдачи средств в сутки и за одну операцию. Так мошенники не смогут снять деньги сверх установленного лимита.
- Закажите себе карту с чипом и магнитной полосой. Такая карта лучше защищена от считывания и подделки путём скимминга.
- В любой непонятной ситуации сразу звоните в свой банк по телефону, указанному на вашей карте, и уточняйте информацию.
- При утере или хищении карты срочно звоните в банк и блокируйте карту.
- Подключите услугу СМС-информирование. С ней вы будете в курсе операций по вашему счету и карте.
- Установите на компьютер и телефон лицензионную антивирусную программу.
- Пользуйтесь банкоматами, установленными в безопасных местах, оборудованных системой видеонаблюдения, охраной.
- Для продажи старых вещей через интернет-площадки используйте номер телефона, не привязанный к мобильному банкингу.

По инициативе прокуратуры Кировской области в период с 15 по 30 сентября 2021 года на территории области, в том числе Нагорского района, организовано проведение мероприятий правового просвещения и правового информирования, направленных на повышение финансовой грамотности населения, предотвращение хищений имущества граждан, в том числе с использованием информационно-коммуникационных технологий.

В рамках мероприятий 24 сентября 2021 года с 10 до 17 часов (перерыв с 13 час. до 13 час. 48 мин.) прокуратура Нагорского района проведёт прием сообщений по телефону «горячей линии».

Все желающие могут сообщить любую информацию о нарушениях в указанной сфере, получить разъяснение законодательства.

Рассматриваться будут все звонки, в том числе и анонимные. Гражданам гарантирована конфиденциальность.

Сообщения можно оставить, позвонив по телефону (883349) 2-19-03, 2-16-50, а также на официальной странице прокуратуры Кировской области Единого портала прокуратуры Российской Федерации, выбрав прокуратуру Нагорского района.

Прокурор Нагорского района

старший советник юстиции А.Е. Ковязина