Полиция предупреждает жителей Матушкино о мошенничествах с банковскими картами и счетами

17.04.2018

Сегодня в повседневной жизни используется множество разнообразных высокотехнологичных устройств - пластиковых карт, мобильных телефонов и компьютеров. Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний. Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, пластиковыми картами и компьютерами.

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

Сообщение «Ваша банковская карта заблокирована».

Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда жертва звонит по указанному телефону, ей сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

На самом деле злоумышленникам нужен номер карты жертвы и ПИН- код. Как только потерпевший их сообщает, злоумышленники получают возможность управлять счетом.

Как избежать мошенничества: не сообщать реквизиты карты никому. Ни одна организация, включая банк, не вправе требовать ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.

Ежегодно возрастает число хищений денег со счетов клиентов банков.

1. Хищения под видом покупки товара по объявлению в Интеренте.

Как это происходит. Законопослушный гражданин размещает объявление о продаже вещей на страницах магазина бесплатных объявлений в Интеренте. Злоумышленник звонит по указанному в объявлении номеру, заверяет, что уже сейчас готов приобрести товар, перечислив деньги на карту банка. Продавец диктует реквизиты карты или счета. Через 15-20 минут злоумышленник вновь перезванивает продавцу, сообщает, что стоит у платежного терминала и не может отправить деньги. Ему нужен СМС-код, который сейчас поступит на телефон продавца (потенциальной жертвы обмана). Если в силу неосведомленности продавец называет этот код, то через несколько секунд ему поступает СМС о снятии всех денег с его счета.

На самом деле злоумышленника не интересуют ваши вещи, он не ходит к терминалу оплаты, а сидит за компьютером и пытается войти в Личный кабинет жертвы по номеру карты. Если при повторном разговоре от наивного продавца он получает СМС-код подтверждения входа в Личный кабинет, то быстро заходит в чужой Личный кабинет и все имеющиеся на счету средства отправляет на свои счета, затем обрывает разговор.

Что делать? При подключении дистанционного обслуживания в банке и пароля для Личного кабинета нужно выяснить, как именно он работает! В дальнейшем никому не сообщать разовые СМС-пароли подтверждения входа в Личный кабинет!

2. Хищений денежный средств со счетов с использованием вредоносных программ.

Вредоносная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в СМС или ММС сообщениях. Одним из признаков наличия вредоносных программы на мобильном телефоне является направление «пустых» СМС или ММС сообщений на телефоны.

Задача такой программы - обеспечить злоумышленнику доступ к устройству жертвы и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений.

Если к смартфону подключена услуга «Мобильный банк», то сведения о доступе в Личный кабинет становятся известны злоумышленнику. Тайно входя в чужие Личные кабинеты, он может перечислять денежные средства сотен потерпевших на свои счета, а затем обналичивать.

Тактика борьбы достаточно проста:

Не допускать, чтобы вредоносные программы попадали на компьютер или смартфон (чаще всего страдают владельцы смартфонов с операционной систмой Андроид). Если они все-таки попали, ни в коем случае не запускать их. Принять меры, чтобы, по возможности, они не причинили ущерба. Использовать специальные антивирусные программы. Если деньги все-таки списались, немедленно прекратить любые действия с сотовым телефоном. Незамедлительно обратиться в свой банк по телефону горячей линии с поручением о блокировке операции с расчетным счетом и отзывом криминального перевода. И с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе «Мобильный банк». В течение одного дня обратиться с заявлением в правоохранительные органы о факте хищения денежных средств.
