Сотрудники полиции УВД по ТиНАО напоминают гражданам как не стать жертвой мошенников при использовании банковских карт

Хищение денежных средств с банковской карты кажется куда сложнее, чем из сумки, кошелька или даже автомобиля. Но, тем не менее, в настоящее время злоумышленники прибегают к различным способам совершения такого вида противоправного деяния.

Какая информация о вашей карте нужна злоумышленникам?

Им нужны реквизиты вашей карты: номер карты, имя и фамилия владельца, срок действия, код проверки подлинности карты (три цифры на обратной стороне, например, CVV или CVC), ПИН-код. Также код из смс для подтверждений платежей и переводов на тех сайтах, где платежи нужно подтверждать с помощью такого кода.

1. Вы платите обычной банковской картой

Злоумышленником может оказаться работник сферы торговли и услуг. Кассир или продавец, принимая для расчета вашу банковскую карту, может сфотографировать нужные данные (номер карты, срок действия, имя владельца и код на обратной стороне), а после расплатиться ей в интернете.

Как предотвратить?

Рассчитываясь, постарайтесь не упускать из вида свою карту. И вводите ПИН-код так, чтобы он не был виден посторонним.

2. Вы платите картой с системой бесконтактной оплаты

Картами с системой бесконтактной оплаты можно расплачиваться мгновенно, в одно касание, если ваш платеж не превышает определенный лимит. ПИН-код при этом вводить не нужно. Злоумышленники могут похитить деньги с такой карты, прислонив считыватель или POS-терминал к сумке.

Как предотвратить?

Чтобы бесконтактная оплата не проходила без вашего ведома, карту лучше хранить в кошельке или в специальном чехле для банковских карт.

3. Вы получили тревожное смс-сообщение или звонок от родственника

С незнакомого номера вам пишет или звонит якобы родственник и говорит, что попал в беду и ему срочно нужны деньги, но времени объяснять ситуацию у него нет. В таких сообщениях часто манипулируют срочностью ситуации, и присылают их в крайне неудобное время, например, ночью.

Как предотвратить?

Не спешите переводить деньги. Попытайтесь выяснить детали — обычно долгие разговоры не входят в планы злоумышленников. Если выяснить ничего толком не удалось, перезвоните родственнику, от имени которого обращаются, чтобы убедиться, он ли вам звонит/пишет.

4. Вам пришло сообщение «от банка»

С незнакомого номера приходит смс-сообщение, что ваша карта заблокирована. В смс указан номер, по которому нужно позвонить для уточнения деталей. Позвонив, вы попадете в фальшивую службу безопасности банка, где вас будут убеждать сообщить данные карты или подойти к ближайшему банкомату и произвести операции. Выполнив указания злоумышленников, вы откроете им доступ к карте, и они украдут ваши деньги.

Как предотвратить?

Не перезванивайте — сперва выясните, действительно ли данное сообщение отправлено банком. Настоящие банки обычно присылают уведомления с одного и того же номера. Кроме того, на вашей карте указан телефонный номер для связи с банком — позвоните по нему и уточните, заблокирована ли она. Или обратитесь к сотрудникам ближайшего отделения банка.

5. Вам звонят из госучреждения

Вам звонят люди и представляются сотрудниками Банка России, прокуратуры, суда, Министерства здравоохранения, Министерства финансов и других учреждений. Они сообщают, например, о положенном возмещении ущерба от действий мошенников: о компенсации за купленные медицинские товары или услуги экстрасенсов. Если для получения обещанной компенсации «сотрудник» попросит вас что-то оплатить (подоходный налог, налог на прибыль, банковский сбор, обязательную страховку, госпошлину, комиссию за перевод денег), а тем более попросит предоставить паспортные данные или банковские реквизиты, это — телефонный мошенник.

Как предотвратить?

Не следуйте указаниям и ничего не оплачивайте. Не предоставляйте личную информацию, у настоящих сотрудников она уже есть.

Защититесь от мошенников:

-Подключите мобильный банк, чтобы отследить операции, которые вы не совершали. Так вы сможете оперативно отреагировать на действия мошенников — а время в этом случае очень важно.

-Не храните крупные суммы денег на карте, которую вы носите с собой и используете для повседневных трат.

-Если вы планируете использовать карту только в России — обязательно сообщите об этом сотрудникам банка.

-Расскажите пожилым родственникам об уловках мошенников — именно они чаще всего становятся мишенью злоумышленников.

Что делать, если вы все-таки столкнулись с мошенничеством?

Если с вашей банковской карты вдруг списали деньги:

-Как можно скорее позвоните в банк (номер есть на обороте карты), сообщите о мошеннической операции и заблокируйте карту.

-Обратитесь в отделение банка и попросите выписку по счету. Напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приеме.

-Обратитесь в правоохранительные органы с заявлением о хищении.

Сотрудники полиции УВД по ТиНАО напоминают всем жителям округа - будьте бдительны и соблюдайте правила личной безопасности! Если Вы стали жертвой мошенников, незамедлительно обращайтесь в полицию по телефону 02 (с мобильного – 102) или по телефону дежурной части УВД по ТиНАО ГУ МВД России по г. Москве: 8 (495) 850-13-20.