ПРОКУРАТУРА РАЗЪЯСНЯЕТ

Самые распространенные способы хищения средств с банковских карт (кардинга) основаны на психологических методах убеждения, обмана или запугивания клиентов. По данным российского Центробанка, среди всех атак более 80% приходится на связанные с социальной инженерией. Наиболее популярен среди мошенников телефонный фишинг— так называют процесс выманивания персональных данных у банковских клиентов.

Как работают мошенники

* Представляясь банковскими сотрудниками («службой безопасности» или «службой финансового мониторинга»), сообщают о подозрительной активности и предлагают продиктовать данные карты, чтобы банк принял меры по защите средств.
* Убеждают перевести деньги на отдельный счет якобы для их защиты, сделать это можно онлайн либо сняв деньги в банкомате — в этом случае клиенту даже могут заказать до него такси.
* Просят установить специальное программное обеспечение для «защиты средств», с помощью которого мошенники могут украсть данные карты и оформить предодобренный кредит, после чего вывести средства.
* С начала пандемии мошенники активно эксплуатируют тему коронавируса, будь то «бесплатная» диагностика, медицинская помощь, пособия, компенсации, возврат средств за авиабилеты и другие предлоги, конечной целью которых является перевод денег.
* Сообщают пожилым людям о положенных выплатах от имени сотрудников Пенсионного фонда, в этом случае узнать номер банковской карты и другие данные им нужно якобы для перечисления денег. В некоторых случаях злоумышленники предлагают перевести деньги на сторонний счет для уплаты госпошлины за будущую компенсацию.

**Важно! Не стоит сообщать третьим лицам данные карты, в том числе четырехзначный PIN-код и трехзначный CVC-код, указанный на обороте. При звонках от мошенников могут отображаться реальные номера банковских телефонов. Они могут представляться также полицейскими или работниками бюро кредитных историй.**

Почтовый фишинг, соцсети и поддельные сайты

Рассылаемые мошенниками письма могут содержать ссылки на поддельные сайты, имитирующие странички интернет-магазинов с большими скидками, а также отелей, сервисов по продаже авиабилетов, страховых компаний, различных ведомств. Письма приходят также под видом квитанций об оплате коммунальных платежей или в виде официальных уведомлений от банков и других организаций.

Еще один популярный способ мошенничества связан с продажами на сайтах объявлений, где покупатель по поддельной ссылке вводит данные для оплаты несуществующего товара.

В соцсетях мошенники делают рассылки по списку друзей со взломанного аккаунта с просьбой перевести денег на карту. Подобную информацию всегда необходимо перепроверять по другим каналам связи.

**Важно! Не нужно переходить по ссылкам из подозрительных писем и загружать неизвестные программы. Остерегайтесь оплачивать покупки на подозрительных сайтах, не переводите деньги, если нет уверенности в получателе. Контролируйте все операции по счету и пользуйтесь антивирусными программами.**

Прокуратура Сузунского района