«Перевод на «безопасный» счет» - новый вид мошенничества

Киберпреступники придумали новый способ обмана доверчивых граждан. Теперь мошенники звонят своим жертвам и предлагают помощь якобы в спасении денег путем перевода их на «безопасный» счет.

Как пояснил управляющий Отделением Банка России по Чеченской Республике Иса Тамаев, киберпреступники звонят потенциальным жертвам и, представляясь сотрудниками банка, спрашивают, в каком отделении и когда они хотят закрыть счет из-за якобы полученного заявления о совершении данной операции.

- Естественно, человек на другом конце провода отвечает, что никакого заявления он не писал. На что злоумышленники говорят, что держатель банковской карты стал жертвой хакеров и в любой момент может потерять свои сбережения. Чтобы этого не произошло, деньги надо перевести на «безопасный» счет. Для этого лжесотрудник банка просит назвать реквизиты карты, срок действия и трехназчный код на ее обратной стороне. Этих данных мошенникам достаточно, чтобы перевести деньги на свой счет, - объяснил он.

По словам Исы Тамаева, афера в первую очередь рассчитана на доверчивых людей с низким уровнем финансовой грамотности. Примитивная схема мошенников заканчивается неудачей, если на том конце провода откажутся сообщать свои персональные данные.

- Жертвами мошенников чаще всего становятся экономически активные граждане 30–45 лет, в основном это женщины. У них высокий уровень доверия к безопасности современных технологий, - рассказал он.

По данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России, в 2019 году 7 из 10 хищений были совершены с использованием приемов так называемой «социальной инженерии». При этом большая часть денег – около 3 млрд рублей – похищена в результате оплаты товаров и услуг в Интернете.

Управляющий Отделением Банка России по ЧР Иса Тамаев отметил, что современное общество чересчур доверяет социальным сетям, люди склонны выставлять свою жизнь напоказ.

- Когда в открытом доступе публикуется столько информации, преступник без особого труда может узнать фамилию, имя, отчество, место работы, номер телефона потенциальной жертвы. Этих данных уже достаточно, чтобы проводить обзвон. Помните о том, что никому и ни при каких обстоятельствах нельзя сообщать личные данные, реквизиты карты и секретную информацию: CVC/CVV — код на обратной стороне карты, ПИН-код и коды из СМС. Реальный банк никогда не будет у вас спрашивать эту информацию. Поэтому, если вам задают подобные вопросы, сразу прекращайте разговор и связывайтесь со своим банком, - заключил он.