ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

Отделение по Пермскому краю Уральского главного управления
614990, г. Пермь, ул. Ленина, 19

Пресс-релиз

Мошенники придумали новую схему обмана с помощью полиса ОМС

Преступники звонят своим жертвам от имени страховой компании и говорят, что срок их полиса обязательного медицинского страхования (ОМС) якобы истек и убеждают обновить его, выпустив новый – в электронном виде.

Затем они просят человека установить поддельное приложение Минздрава и получают с помощью него удаленный доступ к чужому телефону. Фальшивое приложение содержит вирус – он позволяет преступникам добраться до мобильного банка и счетов жертвы.

Необходимо помнить, что полисы ОМС для граждан страны действуют бессрочно. Менять бумажные или пластиковые документы на электронные не нужно. Но для удобства можно выпустить цифровой полис – это QR-код, который действует точно так же, как обычный полис. Получить его можно через Госуслуги, никакие отдельные приложения при этом скачивать и устанавливать на телефон не требуется.

Если кто-то связался с вами по поводу ОМС, положите трубку и самостоятельно перезвоните в страховую компанию, которая выдала вам полис. Название и контакты организации указаны на самом документе.

Проверяйте любую информацию в официальных источниках. Устанавливать по просьбе незнакомцев мобильные приложения или скачивать по ссылкам какие-то файлы очень опасно, даже если собеседник представился сотрудником страховой, медицинской, любой другой организации или ведомства.

Мошенники стали обманывать военнослужащих и их родных

Злоумышленники обновили свою популярную схему про «безопасный» счет. Теперь они начали использовать ее в отношении военнослужащих либо их близких родственников. Мошенники звонят или пишут своим потенциальным жертвам и сообщают, что единовременная выплата в размере 195 тыс. рублей, которая причитается военным в соответствии с указом Президента РФ, будет удержана из денежного довольствия.

Причина – дисциплинарное взыскание или нарушение при выполнении служебных обязанностей в зоне проведения специальной военной операции (СВО). Для большей убедительности злоумышленники направляют в мессенджер «копию выписки» якобы из приказа Департамента финансового обеспечения Минобороны России. По сценарию, придуманному мошенниками, военнослужащему или его родным, чтобы избежать списания денег и сохранить средства, предлагают перевести все накопления с карты на «безопасный» счет, а затем средства обещают вернуть. Однако, получив обманным путем деньги жертвы, телефонные аферисты исчезают.

«Мошенники постоянно актуализируют свои легенды под актуальную повестку. Чтобы не стать их жертвой достаточно соблюдать несколько простых правил. При поступлении такого телефонного звонка прервите разговор. Если вам пришло подозрительное сообщение или письмо, не реагируйте на них. Следует помнить, что «безопасных» или «специальных» счетов не существует. По любым вопросам, связанным с деньгами, самостоятельно обратитесь в свой банк по номеру телефона, указанному на его официальном сайте или на обороте платежной карты», – отметил управляющий Отделением Банка России по Пермскому краю Алексей Моночков.

С наиболее распространенными мошенническими схемами можно ознакомиться на сайте Банка России (http://www.cbr.ru/information_security/pmp/).

Пресс-служба Отделения Пермь Уральского ГУ Банка России
8 (342) 218-72-30 57media@cbr.ru