ГКУ «Государственное юридическое бюро» в целях предостережения, изучив опыт других регионов, информирует вас о том, что по регионам России участились случаи хищения денежных средств с платежных банковских карт, в том числе путем мошеннических действий в сети интернет, а также посредством использования сотовой связи.

Подготовлена следующая полезная информация. Предлагаем внимательно изучить содержание данной информации и следовать нашим рекомендациям. Они помогут защитить вас от мошеннических действий и сберечь ваши денежные средства.

Основные виды мошенничества в сетях сотовой и беспроводной связи:

1. сотовый беспроводной телефон используется как средство передачи голосовой информации, имеющей подвиды и типы:
- - «ваш сын попал в аварию…»
- - «мама/папа у меня проблемы…»
- - «это из банка/пенсионного фонда, социального страхования…»
- - «ваш родственник задержан, нужна помощь...»

- сотовые телефоны, используемые для передачи через «смс-сообщения» сложной информации:
- - «мама брось мне на этот номер денег, потом все объясню…»
- - «ваша банковская карта заблокирована, подробности по телефону…»
- - «с вашего счета списаны 4000 руб. подробности по телефону…»

Хищение денежных средств с использованием вредоносного программного обеспечения путем заражения мобильных устройств на базе операционных систем Android. Мобильные телефоны используют мошенники для передачи «смс-сообщений» через мессенджеры, такие как Viber, Watsap и др. с вредоносной информацией, например:

- - «здесь наше с тобой фото http://.....»
- - «скачайте уже сегодня техническое обновление для телефона http://…»

- - «ваш аккаунт-страница в VK сломана, пройдите регистрацию http://…»

Также практикуется рассылка «смс-сообщений» со ссылками на интернет-ресурсы, с зараженными ПО лицам, размещающие свои частные объявления на сайтах бесплатных объявлений. Как правило, большинство граждан пользуются приложением к мобильному устройству «Мобильный банк». При заражении мобильного устройства вредоносное ПО осуществляется несанкционированное пополнение абонентского номера потерпевшего с привязанной банковской картой потерпевшего, с последующим переводом денежных средств на счетах других абонентских номеров, как правило, злоумышленников, которым также привязаны банковские карты либо подключена услуга киви-кошелек. Как в первом, так и во втором случае осуществляется вывод денег через банковские карты.

Мошенничество, совершенное в сети интернет, с помощью сети интернет.

1. мошенничество при продаже товаров через интернет-магазины по предоплате, по заранее низким ценам, распространенные виды:
- - продажа телефонов Iphone.
- - цифровой, бытовой техники.
- - элитной одежды, украшений, автомобилей и т.п.

- получение от интернет-магазина, продавца товара.
- хищение денежных средств с банковских карт путем пополнения аккаунта социальных сетей.

ГКУ «Государственное юридическое бюро» обращается ко всем жителям Чеченской Республики, особенно к лицам пожилого возраста: соблюдайте разум, осторожность и бдительность!

После поступления на ваши мобильные телефоны звонков о так называемой помощи, обязательно перезванивайте своим детям и другим родственникам и выясните действительно ли с ними случилась беда.

При получении «смс-сообщений» из фиктивных банков «Ваша карта

заблокирована» ни в коем случае не перезванивайте на указанный в сообщении номер, пользуйтесь номерами горячих линий банков или действующими номерами тех кредитных учреждений, где размещены ваши денежные средства!

Не разглашайте по телефону свои персональные данные: паспорт, адрес проживания!

Не делайте поспешных выводов после полученной информации и не отдавайте преступникам свои денежные средства!

Если вы решили заказать товар через интернет-магазин оформляйте заказ только через проверенный магазин, оплачивайте стоимость товара только после фактического получения! Будьте бдительны, не вступайте посредством мобильной связи в диалог с незнакомыми вами людьми!