



ПРОКУРАТУРА
Хасавюртовского района

Памятка для граждан:

Осторожно мошенники!

По-прежнему на территории республики сохраняется тенденция к увеличению числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Однако самыми распространенными дистанционными преступлениями являются хищения.

Мошенники очень хорошо знают психологию людей и умело используют всю доступную информацию, включая ту, что жертва мошенничества невольно выдает при общении.

Основные способы действия мошенников:

✓ Вам пришло СМС-сообщение или поступил звонок якобы от работника банка о том, что Ваша банковская карта заблокирована, произошло списание денежных средств, или необходимо подключить какую-нибудь услугу?

✓ Не выполняйте никаких операций с картами по полученным от неизвестных лиц инструкциям по телефону, сразу же обратитесь в отделение банка или по телефону «горячей линии».

✓ Вам отправили сообщение или позвонили, якобы Ваши близкие, или от имени сотрудников полиции и сообщили, что родственник попал в беду и требуют деньги для решения проблем?

✓ Прекратите разговор, перезвоните своим близким и убедитесь в достоверности информации.

✓ Вам позвонили по объявлению, размещенному Вами на сайтах «Авито» и др., и просят для перечисления денежных средств подойти к банкомату и выполнить какие-либо операции по карте?

г. Хасавюрт
2024

Помните, что для перечисления денежных средств на Вашу карту достаточно знать только ее номер. Не сообщайте никому другой дополнительной информации (реквизиты, пароли, коды доступа) и не подключайте дополнительную услугу «Мобильный банк» к чужому номеру.

✓ Вам от друзей поступило обращение на интернет-сайтах («Одноклассники», «В Контакте» и др.) с просьбой занять деньги или назвать реквизиты своей карты?

В данном случае от имени друзей могут действовать мошенники, цель которых одна – завладеть Вашими деньгами.

✓ Вам предлагают приобрести товар в Интернет-магазине?

Убедитесь, что это не мошенники, не приобретайте товары в сомнительных Интернет-магазинах. Производите оплату только при получении товара.

«Схемы», используемые злоумышленниками для хищения денежных средств граждан с банковских карт:

❖ Мобильный банк:

при установке приложений из интернета необходимо быть осторожными. Дело в том, что создатели программы специально заражают ее вирусом, который, проникая в смартфон, начинает работать на мошенников. Он заменяет окно мобильного банка поддельным, а владелец телефона вводит туда свои данные, ничего не подозревая. Вирус отправляет их мошенникам, которые затем незаконно получают доступ к карточному счету клиента. Для того, чтобы предотвратить такие махинации с банковскими картами устанавливайте только лицензионные приложения.

а также антивирусные программы, а также периодически проверяйте количество денег на вашем счету.

❖ С помощью беспроводного терминала и бесконтактной технологии PayPass:

злоумышленники снимают деньги у пассажиров с помощью беспроводного терминала через одежду и стенки сумок. Посредством бесконтактной технологии PayPass с карточки без PIN-кода можно снять до 1000 российских рублей. Чтобы снять деньги со счета, достаточно приложить устройство к карману или сумке, считыватели бесконтактных карт работают на расстоянии до двадцати сантиметров, достать их проблем не составляет.

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ ОБМАНА НЕМЕДЛЕННО СООБЩИТЕ В ПОЛИЦИЮ!