

В случае если имеются основания полагать, что в отношении Вас предпринимаются мошеннические действия, либо Вы уже стали жертвой мошенничества, необходимо незамедлительно обращаться в правоохранительные органы по телефонам:

**02, 112**

**БУДЬТЕ БДИТЕЛЬНЫ!**

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПРОКУРАТУРА МУРМАНСКОЙ  
ОБЛАСТИ

ПРОКУРАТУРА ГОРОДА  
СЕВЕРОМОРСКА



МОШЕННИКИ: КАК НЕ ПОПАСТЬ  
В ПРЕСТУПНУЮ ЛОВУШКУ  
ТАКТИКА МОШЕННИКОВ  
КАК РЕАГИРОВАТЬ

2023



В последнее время распространен вид мошенничества, при котором злоумышленники звонят людям под видом сотрудников службы поддержки оператора сотовой связи, сообщая, что номер абонента скоро перестанет действовать.

Чтобы избежать этого, предлагается набрать на телефоне комбинацию цифр. В результате подключается переадресация звонков и текстовых сообщений, в том числе с смс-кодами от банка, на номера мошенников. Это позволяет получить доступ к дистанционному управлению банковским счетом и похитить деньги.

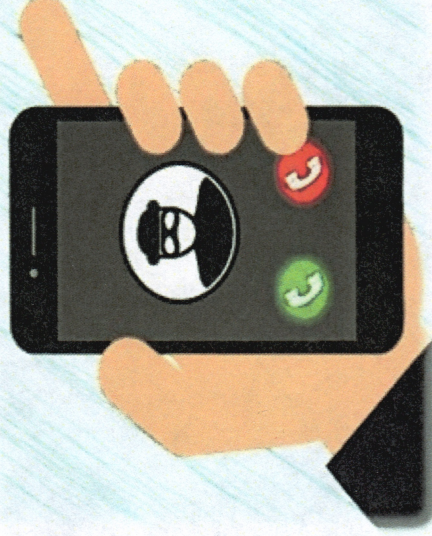
Мошенники могут использовать разные легенды – сообщить, что необходимо переоформить договор об оказании услуг связи, поменять тарифный план на более выгодный, отключить платную услугу, сменить мобильного оператора с сохранением номера.



Независимо от причины звонка, цель мошенников – получить у человека код для входа в его личный кабинет мобильного оператора и установить переадресацию, либо подключить ее самостоятельно.

Если Вам позвонили с такими предложениями:

- прервите разговор;
- позвоните в службу поддержки мобильного оператора по номеру, который указан на официальном сайте.



Мошенникам все сложнее обходить анти-спам фильтры, которые предупреждают людей о подозрительных звонках.

Преступники переходят на мессенджеры, в которых такой защитной системы нет. Номер абонента обманщики скрывают, а на аватар ставят логотипы известных банков, чтобы вызвать доверие людей.

Обращаем внимание, что секретные данные нельзя сообщать никому, даже представителям банка!



Клиенты банка берут трубку, когда видят знакомый логотип.

Злоумышленники представляются сотрудниками банка и под разными предлогами выманивают конфиденциальную информацию: реквизиты карт, логины и пароли от онлайн-банка, коды уведомлений об операциях.

В итоге мошенники получают доступ к банковским счетам.