**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ**

**(БАНК РОССИИ)**

**Отделение по Пермскому краю Уральского главного управления**

614990, г. Пермь, ул. Ленина, 19

[www.cbr.ru](http://www.cbr.ru)

**Пресс-релиз**

**Остерегайтесь звонков мошенников под видом сотрудников службы сотовой связи**

Злоумышленники звонят людям под видом техподдержки оператора мобильной связи и сообщают, что номер абонента вскоре будет отключен. Чтобы этого не случилось, человеку предлагают набрать на телефоне определенную комбинацию цифр. В результате он подключает переадресацию звонков и текстовых сообщений на номера злоумышленников. Им также начинают поступать смс-коды от банка, которые позволяют получить доступ к дистанционному управлению банковским счетом и похитить деньги.

Мошенники могут также сообщить, что необходимо переоформить договор об оказании услуг связи, поменять тарифный план на более выгодный или предлагают отключить платные и не нужные услуги. Иногда они говорят, что поступила заявка о смене мобильного оператора с сохранением номера.

Цель мошенников – либо получить у человека код для входа в его личный кабинет мобильного оператора и установить переадресацию, либо убедить абонента подключить ее самостоятельно.

Если вам позвонили с такими предложениями, прервите разговор. Самостоятельно позвоните в службу поддержки мобильного оператора по номеру, который указан на его официальном сайте.

Больше о популярных среди мошенников схемах и о том, как противостоять им, можно узнать в специальном разделе на [сайте](https://cbr.ru/information_security/pmp/) (<https://cbr.ru/information_security/pmp/>) Центрального банка РФ.

**Последние распродажи закрывающихся компаний**

Мошенники используют ситуацию с уходом из России популярных брендов, которые устраивают распродажи остатков своих товаров. Аферисты представляются в соцсетях и мессенджерах сотрудниками таких компаний и предлагают оформить заказы со скидками и без очередей. А на самом деле воруют деньги и данные карт.

Для правдоподобности злоумышленники сообщают, что якобы работникам компании дают особые бонусы за объемы продаж и привлечение покупателей.

Человека просят прислать страницу официального сайта компании или магазина с описанием нужного товара либо просто его название или фото. Взамен мнимый сотрудник присылает ссылку на корзину с уцененным товаром и предлагает закончить оформление заказа.

На самом деле ссылка мошенников ведет на фишинговый сайт, адрес которого отличается от настоящего парой символов. При этом дизайн сайта может в точности повторять оригинальный. Как только покупатель вводит реквизиты своей карты, чтобы оплатить товар, его деньги и данные попадают к преступникам. Затем они могут полностью обнулить карточный счет покупателя. В этом случае банки не компенсируют потери.

Будьте внимательны не попадайтесь на уловки аферистов!

*Пресс-служба Отделения Банка России по Пермскому краю*