

Мошенничества, связанные с темой «Почты России».

Самый распространенный сценарий мошенничества в этом направлении на сегодняшний день предполагает телефонный звонок российским гражданам, который якобы исходит от работников «Почты России» или же каких-то других почтовых служб.

Во время такого звонка, если пользователь сразу не кладёт трубку, аферист заявляет о том, что человеку якобы поступила посылка из-за рубежа, за которую требуется перечислить таможенный сбор.

В этом случае многие граждане сообщают мошенникам, что они никакой посылки из-за рубежа не заказывали и не ждали. Тогда аферисты сообщают, что для отмены посылки и для того, чтобы не платить таможенный сбор, необходимо продиктовать код из SMS-сообщения, который придёт на телефонный номер абонента.

В действительности же в этот момент на телефонный номер потенциальной жертвы приходит SMS-сообщение с кодом подтверждения.

Однако этот код мошенники запрашивают, чтобы получить доступ к личному кабинету пользователя в онлайн-банкинге или же к аккаунту на портале госуслуг и других популярных сервисов, где содержатся чувствительные данные.

Чтобы не стать жертвой таких киберпреступлений необходимо оставаться максимально бдительными и критически оценивать любые запросы на передачу конфиденциальных данных или персональной информации, которые поступают от неизвестных лиц по телефону, в социальных сетях и мессенджерах.

Представители государственных органов, «Почты России» и других учреждений никогда не будут запрашивать логины, пароли, коды подтверждения из SMS-сообщений и другие идентификационные данные.

[#МВДРоссии](#) [#МВД](#) [#МВД74](#) [#Полиция74](#) [#Челябинскаяобласть](#) [#ПолицияЮжногоУрала](#) [#полицияКатавИвановскийрайон](#) [#Профилактика](#) [#Мошенничество](#)

