НЕ ВЕРЬ, НЕ БОЙСЯ, НЕ КЛИКАЙ

Как работают новые схемы онлайн-мошенников. Комментируют эксперты РОЦИТ

РОЦИТ

СМС
от «Роскомнадзора»

Жителям Херсонской области и ряда других регионов стали приходить тревожные СМС якобы от Роскомнадзора. В сообщении говорится, что входящий звонок был прерван по подозрению в мошенничестве, а для подтверждения безопасности нужно срочно перезвонить по указанному номеру.

На первый взгляд – забота о вас, но на деле – хорошо замаскированная ловушка. Так мошенники вынуждают вас самим выйти на связь, думая, что вы спасаете себя от обмана, хотя все наоборот.

Как не попасть в руки преступников:

Запомните, что Роскомнадзор не разъединяет звонки, не рассылает сообщения и никогда не звонит гражданам. Такие СМС – фикция, рассчитанная на панику и спешку. Перезвонив, вы попадаете прямо в руки преступников.

Фальшивые Telegram-боты служб доставки

Вам звонят через мессенджер от имени «Почты России» или другой логистической компании и сообщают о проблеме с посылкой. Решить можно просто – пройти авторизацию в «официальном» Telegram-боте. Бот выглядит солидно: логотип, имя бренда, даже язык общения корректный.

Что будет, если ввести данные?

Но как только вы вводите туда свои данные – вы передаете их напрямую мошенникам. Особенно опасно, если вы указываете логин и пароль от «Госуслуг» или банковских приложений.

В лучшем случае это закончится спамом. В худшем – потерей доступа к личным кабинетам и денег со счетов.

«Безопасный счет» с новым названием

Преступники продолжают использовать прием с переводом средств на так называемый безопасный счет, но при этом используют иные формулировки, чтобы не вызывать подозрений.

Теперь же вместо слова «безопасный» используют более изощренные термины: «декларационный», «секретный», «резервный», «транспортировочный», «криптовалютный» – не суть, главное, чтобы звучало серьезно.

Цель злоумышленников

В каждом случае цель одна – убедить жертву, что перевод на этот счет обезопасит ее финансы в случае угрозы.

На деле такие счета принадлежат злоумышленникам, и все переведенные деньги теряются безвозвратно.

Единственным по-настоящему безопасным счетом остается только ваш собственный.

Простые правила против хитрых схем

Мошенники постоянно используют знакомые образы – названия госструктур, логотипы известных компаний и привычные формулировки, чтобы вызвать доверие и спровоцировать быстрые действия.

Если получили СМС от «Роскомнадзора» или другого госоргана – не перезванивайте. Ни одна госструктура не рассылает такие сообщения и не общается через мессенджеры.

Простые правила против хитрых схем

Не спешите вводить свои данные, если увидели ссылку на Telegram-бота от службы доставки.

Даже если бот выглядит официально, лучше сначала проверить, есть ли он на сайте компании.

И уж точно не переводите деньги на «секретные», «резервные» или «антикризисные» счета – это просто красивая обертка для старого обмана. *Безопасен только тот счет, который вы открыли сами и точно знаете, кому он принадлежит.*