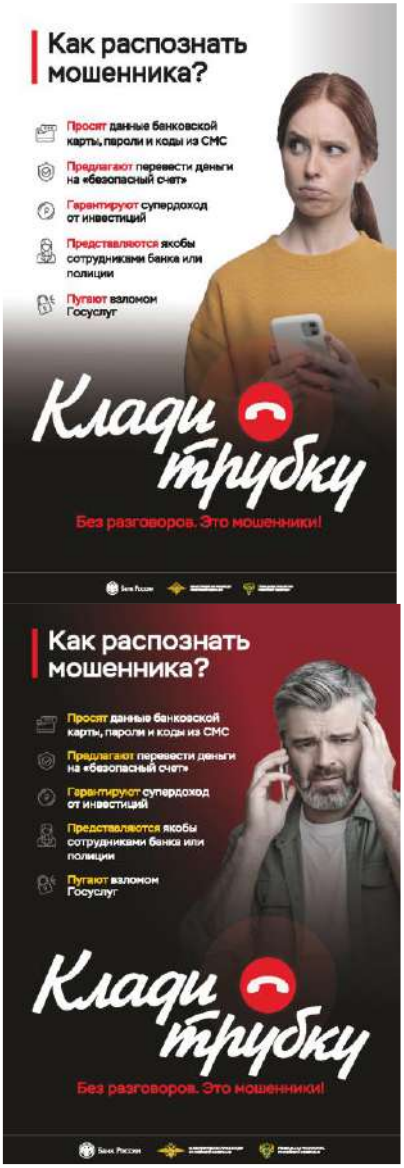
КАМПАНИЯ ПО КИБЕРГРАМОТНОСТИ "КЛАДИ ТРУБКУ"!



В 2024 году проблема мошенничества с использованием методов социальной инженерии остается актуальной, злоумышленники постоянно совершенствуют схемы обмана граждан. Банком России совместно с другими федеральными органами исполнительной власти осуществляется деятельность по противодействию мошенничеству на финансовом рынке, в рамках которой до конца текущего года проводится информационная кампания (далее – ИК) «Клади трубку».

Цель кампании - напомнить гражданам о том, что телефонный звонок – ключевой инструмент мошенников, которые занимаются хищением денежных средств. Они постоянно придумывают все более изощренные схемы и сценарии для звонка, чтобы заполучить доступ к деньгам.

Схемы злоумышленников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Чтобы вызвать доверие, они могут обращаться по имени и отчеству. С первых минут разговора мошенники начинают давить авторитетом и должностью. Следуя общим правилам поведения с кибермошенниками, вы сможете себя обезопасить:

− не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и другие) и финансовые (номер, срок действия, трехзначный код с оборотной стороны карты) данные. Переданные мошенникам личные и финансовые данные могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;

− установите антивирусные программы на все свои гаджеты. Данное ПО предупредит вас в случае установки подозрительного продукта на ваш гаджет. Важно регулярно обновлять антивирусную базу.

− не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, а звонки на неизвестные пропущенные телефонные номера могут быть чреваты как минимум списанием значительной суммы с вашего мобильного счета, а как максимум − быть поводом для мошенников активизировать против вас мошенническую схему;

− не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы.

Сомнительные ссылки могут быть опасны для вашего гаджета наличием вируса или вредоносного ПО на сайте, на который они ведут, а скачивание программ с неофициальных источников может дать мошенникам доступ к вашему гаджету;
− заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получат доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней.

В Центробанке перечислили 8 самых популярных фраз телефонных мошенников, после которых нужно сразу прекращать разговор. Услышав их, лучше самостоятельно перезвонить в указанную организацию.

«Аферисты часто пользуются такими фразами, как «оформлена заявка на кредит», «сотрудник Центробанка», «специальный или безопасный счет», «идут следственные действия, помогите задержать мошенников и не разглашайте информацию», «ваши деньги пытаются похитить, зафиксирована подозрительная операция» и «вас беспокоит специалист финансовой безопасности, сотрудник службы безопасности банка». Также они могут сообщить, что «истекает срок действия SIM-карты» и попросить «продублировать код из SMS-сообщения», – отметили в Центральном Банке России.

УВАЖАЕМЫЕ РЕБЯТА И РОДИТЕЛИ! БУДЬТЕ ВНИМАТЕЛЬНЫ!!!