Приложение к письму

от\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_

**МОШЕННИКИ ИСПОЛЬЗУЮТ SWIFT В НОВЫХ СХЕМАХ ОБМАНА**



Россиянам предлагают перевести их сбережения на якобы безопасные счета. Роскачество рассказывает, какие уловки используются и как не стать жертвой.

**ОТКЛЮЧЕНИЕ SWIFT КАК ПОВОД ДЛЯ МОШЕННИКОВ**

Сообщения о скором или уже состоявшемся отключении SWIFT и о возможном отключении России от международных финансовых операций вызывают много противоречивых эмоций у россиян. Отсутствие понимания того, что эта аббревиатура означает, что за ней скрывается и как эта система связана с банковскими счетами и платежными возможностями, дает повод мошенникам использовать ее в своих новых схемах манипулирования людьми. Мошенники выходят на связь с держателями банковских карт и через активные навыки социальной инженерии «объясняют» доверчивым пользователям, чем им грозит отключение SWIFT.

Самая распространенная схема на сегодняшний день – звонок мошенников якобы из банка с сообщением, что после отключения России от SWIFT, вы потеряете все свои накопления. Для спасения средств необходимо срочно совершить перевод в другой банк или на специальный «защищенный» счет, который уже любезно подготовлен «сотрудником».

**МОШЕННИКИ МОГУТ ПОДМЕНЯТЬ НОМЕР**

Мошенники с помощью специальных сервисов IP-телефонии могут подменять номер, который будет выглядеть как номер вашего банка. Чтобы не попасться на удочку, рекомендация одна: при малейших подозрениях прерывайте разговор и самостоятельно перезванивайте по номеру, указанному на обратной стороне карты. Также не рекомендуется перезванивать на незнакомые номера, особенно на короткие, городские, с кодом, отличным от +7 и начинающимся на 8-809 (номера для оказания платных услуг).

Уловки телефонных мошенников часто могут быть успешны, потому что вы не видите, с кем разговариваете, а фокусируетесь только на голосе звонящего, который путем мастерской манипуляции, интонациями и давлением на эмоции может заставить ваше воображение нарисовать любую желаемую мошенником картину.

**РЕКОМЕНДАЦИИ ОТ РОСКАЧЕСТВА**

Лучшим вариантом будет сразу прервать разговор, как только у вас возникнут хоть малейшие сомнения или вы услышите уже заезженную схему, когда звонивший представляется представителем «службы безопасности банка».

* Помните, что **ни сотрудники банков, ни сотрудники полиции не обзванивают людей** с целью рассказать о проблемах с платежными системами. При сомнительных действиях по картам сотрудники банка просто блокируют карту без каких-либо телефонных уведомлений.
* **Не доверяйте входящим звонкам от незнакомцев**, даже если звонят с номера вашего банка. Подменить номер с помощью специальных сервисов IP-телефонии сегодня просто как никогда.
* Если у вас закралась хотя бы малейшая тень сомнения, что вас хотят обмануть, **кладите трубку**. Звонящий сразу начинает давить на эмоции? Говорит, что вы все потеряете / вам нужно перевести деньги на защищенный счет / установить безопасное приложение на свой телефон / продиктовать код из СМС? Кладите трубку.
* **Ничего не диктуйте по телефону** незнакомому человеку, даже если он представился сотрудником банка или правоохранительных органов. Кладите трубку и перезванивайте сами по номеру на обороте карты или номеру полицейского участка.

https://rskrf.ru/tips/eksperty-obyasnyayut/swift/