КАК ЗАЩИТИТЬСЯ ОТ КРАЖИ ДЕНЕГ С КАРТЫ

Мошенники умеют не только незаметно воровать телефоны и кошельки, но и уводить деньги с банковских карт. Они придумали для этого множество хитрых способов. Чтобы не попасть в ловушку мошенника, нужно всегда соблюдать семь важных правил.

Правило № 1. Никому не сообщайте свои пароли и коды

ПИН–код от карты – это секрет, который никому нельзя раскрывать. Лучше не сохранять его в телефоне и тем более не записывать на карте. А при вводе ПИН–кода в банкомате или в магазине надо всегда прикрывать клавиатуру рукой.

На обратной стороне карточки есть CVC/CVV–код – три секретные цифры. Они нужны для оплаты покупок в интернете. Чтобы мошенники не смогли потратить деньги с вашей карты, ни в коем случае не диктуйте и не показывайте никому CVC/CVV–код.

Сотрудники банка никогда не спрашивают код с карты, ПИН–код, а также коды из СМС, которые присылает банк. Секретными кодами интересуются только мошенники. Обманщик готов прикинуться кем угодно, лишь бы их выведать: не только работником банка, но и родственником, другом или даже незнакомцем, попавшим в беду.

Пример: Звонит незнакомец, извиняется и говорит, что случайно указал ваш номер телефона в какой-то анкете. Он просит продиктовать ему код, который по ошибке пришел вам в СМС. Это точно мошенник. Немедленно бросайте трубку.

Мошенники могут притворяться, что они ваши знакомые, которые якобы хотят скинуть деньги вам на карту. Но для перевода им нужны номер карты, срок ее действия и CVC/CVV–код. Это тоже обман. Для того, чтобы перечислить деньги, достаточно номера карты. Никакие другие данные – срок действия, имя владельца или код – не требуются.

Правило № 2. Подключите СМС–оповещения по карте

Это нужно, чтобы сразу же получать от банка СМС обо всех действиях по карте. Например, обо всех покупках, которые оплачены картой. Эти сообщения нужно читать очень внимательно. Если пришло сообщение о покупке, которую вы не совершали, скорее всего, картой воспользовался мошенник.

Стоит сразу позвонить в банк, сообщить о подозрительном СМС и попросить заблокировать карту. Номер горячей линии банка есть на обратной стороне карты. Лучше всего сохранить этот номер в контактах на своем телефоне и в случае проблем с картой звонить только по нему.

Пример: Пришло сообщение, что с вашей карты списали 1000 рублей за неизвестную покупку. И тут же приходит СМС «из службы безопасности», что «по карте проходит подозрительная операция». Чтобы «ее отменить», просят перезвонить по незнакомому номеру телефона или перейти по ссылке. Упс, это снова обман. Не стоит этого делать: по ссылке, скорее всего, вирус, а номер телефона принадлежит мошенникам.

Правило № 3. Пользуйтесь антивирусами

Очень важно установить антивирусные программы на всех устройствах, которыми вы пользуетесь, – на компьютере, планшете и мобильном телефоне. Антивирус защитит от вредоносных программ и сайтов, с помощью которых мошенники крадут деньги.

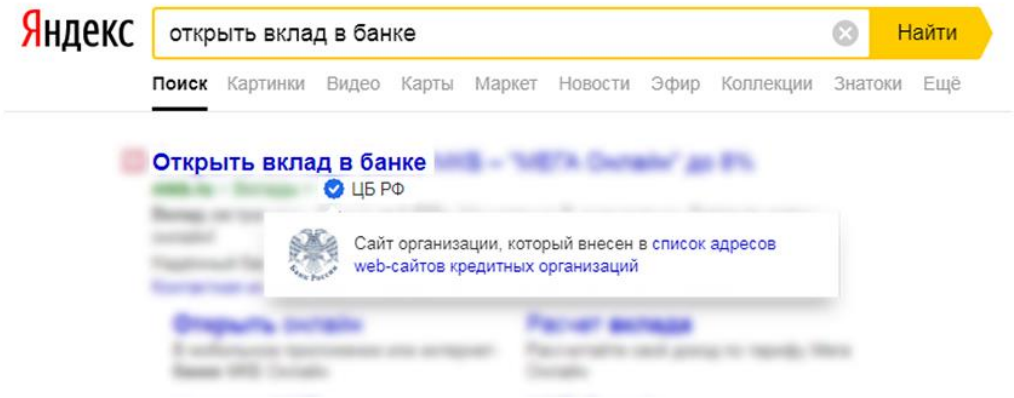
В интернете можно найти бесплатные версии антивирусных программ с ограниченным функционалом. Главное – скачивать их из официальных магазинов приложений или на сайтах известных разработчиков антивирусов.

Правило № 4. Выбирайте безопасные сайты

Мошенники создают сайты–двойники популярных онлайн–ресурсов. Например, они могут сделать копию сайта банка или вашего любимого онлайн–магазина. Если вы введете там свои пароли, коды, данные карты, то они попадут к мошенникам.

Как проверить сайт?

- Сайты банков можно легко проверить с помощью поисковых систем «Яндекс» и Mail.ru. Настоящие сайты реальных банков имеют специальную отметку — галочку в синем кружке. Если такого значка нет – это сайт мошенников.



- Обычно название сайта–двойника почти полностью совпадает с названием какого–нибудь известного сайта, не считая пары букв. Поэтому нужно всегда тщательно проверять адресную строку своего браузера. Набирайте адрес сайта вручную, а лучше сразу сохраняйте официальные и проверенные сайты в закладках.
- Обратите внимание на адрес ресурса. У безопасного сайта он начинается с https://. В конце адресной строки защищенного сайта есть значок в виде закрытого замка. Если сайт не имеет защиты, на нем нельзя вводить личную информацию и данные карты.

Прежде чем вводить данные карты или паспорта на каком–либо сайте, важно внимательно изучить его, почитать отзывы в интернете.

Правило № 5. Не оплачивайте покупки с чужих гаджетов

Делать покупки, заходить на сайт банка или в банковское приложение надо только с личного компьютера, планшета и телефона. Установите пароли на все свои гаджеты.

Если потеряете телефон или планшет, на которых было банковское мобильное приложение и куда приходили уведомления и пароли, срочно звоните в банк. Попросите отключить от этого номера телефона все услуги

и заблокировать доступ к счету с потерянного гаджета. Поменяйте логин и пароль от личного кабинета в интернет–банке.

Когда вы восстановите свой номер у мобильного оператора, можно будет снова подключить к нему СМС–уведомления.

Правило № 6. Не переходите по сомнительным ссылкам из сообщений

Никогда не переходите по ссылкам из писем и СМС от незнакомцев. Это может быть вредоносная программа, которая крадет персональные данные.

Но даже если ссылку прислал кто–то из друзей, не спешите ее открывать. Мошенники могли зайти в чужой аккаунт и разослать сообщения от имени знакомого.

Пример: В соцсети приходит сообщение от друга: «Смотри, фотки с моего ДР! Они просто огонь!». К сообщению прикреплена ссылка или файловый архив. Не стоит сразу по ним кликать. Лучше позвонить другу или написать в другой социальной сети и уточнить, не спам ли это.

Обычно за подобными ссылками и архивами скрываются троянские программы. Они сами устанавливаются на гаджет, воруют и подделывают ваши данные, в том числе могут переводить мошенникам деньги с ваших счетов.

Правило № 7. Перепроверяйте информацию

Мошенники очень надеются, что вы им сразу поверите. Они специально торопят вас, чтобы не дать времени перепроверить информацию. Но в денежных вопросах нельзя спешить.

Чаще всего мошенники используют такие схемы:

- Звонит незнакомец и сообщает, что ваши родственники или друзья попали в беду. Мошенник попросит срочно перечислить деньги, чтобы их выручить. Он надеется, что вы испугаетесь и поведетесь на обман. Не спешите переводить деньги: сначала позвоните родным или друзьям и проверьте, все ли у них в порядке.

- Приходит СМС о том, что вам зачислены деньги. Сообщение похоже на уведомление от банка. Тут же звонит какой–то растяпа, говорит, что по ошибке перевел деньги, и просит их вернуть. Просто бросайте трубку. Скорее всего, это мошенник, деньги вам не приходили, а СМС «от банка» – липовое. Позвоните в банк и спросите, приходили ли деньги на счет. А лучше сообщите родителям и попросите помочь вам разобраться.
- Знакомая, с которой вы давно не общались, внезапно пишет в соцсети и спрашивает, как дела. Завязывается переписка, во время которой она неожиданно просит одолжить ей денег. Это сразу должно насторожить. Скорее всего, аккаунт вашей знакомой взломали. И мошенника вовсе не интересует, как у вас дела, – ему нужны ваши деньги. Ни в коем случае ничего не переводите. Напишите знакомой в другой мессенджер или позвоните и уточните, действительно ли ей нужна помощь. Если это обман – пометьте сообщение как спам и напишите жалобу администрации соцсети.

Не забывайте, что мошенники постоянно изобретают новые схемы обмана.

Пример: «Участвовала в конкурсе в соцсети Instagram около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала вещь, написала организаторам, после чего мне предложили оплатить доставку в размере 450р. После этого мне предложили <u>перейти по ссылке…</u>»

Ни в коем случае никому не передавайте секретную информацию по карте – даже тому, кто представился сотрудником банка. Никогда не переводите деньги, пока не разберетесь в ситуации. Расскажите о случившемся родителям. Перезвоните в банк самостоятельно по официальному номеру горячей линии и уточните интересующую вас информацию. Главное – не спешите.

Ссылка на источник: https://fincult.info/