

Кто караулит вас в интернете, чтобы обмануть и оставить без денег.

Представьте: вам звонят из банка и говорят, что по вашей карте прошла подозрительная операция, сняли несколько тысяч рублей. Вы в панике — деньги нужно спасать. К счастью, сотрудник банка уточняет, что операцию можно отменить. Для этого нужно продиктовать ему номер и срок действия карты.

Знакомьтесь, это мошенник. Он обманывает людей по телефону, чтобы выяснить данные карты и купить по ним айфон. Такие, как он, используют множество схем, чтобы обокрасть людей. В этой статье мы расскажем о некоторых.

На всякий случай напоминаем, что все эти схемы — уголовно наказуемые преступления. В каждом банке есть специальные люди, которые превращают таких героев фишинга в героев тюремных камер.

Хакер

Хакер не вступает в контакт с жертвой. Чтобы собрать нужную информацию — данные карты и коды из СМС — он пишет и распространяет вирусы и зловерные страницы в интернете.

Заразиться легко: достаточно перейти по непроверенной ссылке, и вредоносная программа уже загружается на ваш компьютер. Таких ссылок полно на порносайтах и страницах, где предлагают бесплатно скачать фильмы, книги и музыку. Вы думаете, что загружаете свежий хит Фаррелла Уильямса, а это вирус. Зажали 15 рублей музыканту — отдадите все деньги хакеру, такая вот справедливость.

Если не хотите оценить профессионализм хакера, не стоит переходить по таким ссылкам.

Вирусы приводят вас на страницы, подготовленные мошенниками. То есть вы набираете в адресной строке известный вам сайт, а браузер открывает страницу-клон. Вы думаете, что сайту можно верить и оформляете там покупку, а на самом деле дарите мошенникам данные карты, а следом и код из СМС.

Некоторые вирусы считывают и передают хозяину всё, что жертва вводит с клавиатуры, в том числе секретные данные и пароли.

Вирусами заражают и смартфоны. Это значит, что мошеннику еще проще получить доступ к СМС, которые вам отправил банк. К тому же распознать поддельную страницу на маленьком экране смартфона сложнее: адрес сайта не виден, можно не заметить что-то подозрительное, да и мобильные браузеры защищают хуже, чем настольные.

На беду хакеров, не во всех российских тюрьмах есть компьютеры.

Актер

Если вы не уберегли информацию о себе, мошенник знает ваше имя и номер телефона. После

этого вам поступает звонок от «сотрудника банка». На сцену выходит актер.

Актер называет вас по имени и разыгрывает представление. Например, говорит, что в банке технические проблемы и нужно подтвердить ваш номер телефона. Или представляется сотрудником службы безопасности и сообщает о подозрительной транзакции. Клиент паникует и раскрывает мошеннику данные карты. По ней оформляют покупку, а по телефону просят назвать пароль, который придет по СМС.

К сожалению, актерские навыки не очень полезны в тюрьме.

Почтальон

Почтальон помогает хакеру и актеру, приводит к ним жертву. Загляните в папку «Спам» своего ящика, чтобы посмотреть на письма от такого почтальона. Обычно они сулят подарки, легкие деньги или помощь в погашении кредита — достаточно перейти по ссылке и ввести данные карты, на которую упадет богатство.

Иногда письма приходят якобы от банков, платежных систем или онлайн-сервисов. Часто такие сообщения тревожные: например, говорят, что счет заблокирован и нужно срочно подтвердить личные данные.

Расчет на то, что жертва испугается и откроет прикрепленный файл

Иногда, наоборот, обещают выгоду: например, просят подтвердить поступивший платеж. В любом случае жертву ведут по ссылке и просят ввести реквизиты карты или заражают компьютер вирусом из приложенного файла.

Почтальон ловит жертву, которая поведется на халеву.

По схожей схеме работают СМС, в которых пишут о происшествиях с картой, например, о снятии нескольких тысяч рублей. В конце добавляют: «если вы не совершали операцию, позвоните по номеру ...». Клиент в панике звонит и попадает к актеру, который выясняет всё о карте жертвы. В спешке человек может не заметить ошибку в имени отправителя: кто сходу отличит, например, Ralffeisen от Raiffeisen?

Еще одна попытка напугать получателя. Мошенник надеется, что жертва бросится звонить по номеру из СМС и не заметит ошибку в названии банка.

Увы, почта в тюрьме по расписанию.

Социальный инженер

Социальный инженер — психолог и манипулятор. Его среда — социальные сети и мессенджеры. Через них не только распространяют вредоносные ссылки, но и напрямую выспрашивают секретные данные.

Подделка страницы банка – любимый трюк социального инженера. От лица банков вступают в переписку с людьми и выясняют данные карт. При этом либо ссылаются на технические проблемы, либо предлагают помощь в выплате кредита. Могут прикинуться известным брендом и пообещать подарок: бесплатные билеты от авиакомпании или 20-процентную дисконтную карту в магазине одежды.

Также социальные инженеры пишут людям от лица их друзей. Для этого даже необязательно взламывать страницу: мошенник выбирает человека, ставит его фото себе на аватар, меняет имя и пишет его друзьям. Большинство не полезет проверять страницу отправителя и не заметит подмены.

Самый топорный сценарий: друг за городом, позвонить не может, просит срочно прислать денег. Причем на номер или счет, почему-то вам неизвестный.

От лица друзей просят деньги для какой-то экстренной нужды, выманивают секретную информацию – например, номер карты, чтобы вернуть несуществующий долг, – а также рассылают вредоносные ссылки, по которым якобы находится какой-то интригующий контент.

По ссылке – целый клон YouTube. Но видео он не покажет: нужно «обновить Flash Player». Если скачаете «обновление», поймаете вирус.

Чтобы обмануть человека, необязательно прикидываться его знакомым. Иногда мошенники пишут от лица людей, которым нужна помощь, или предлагают быстрый и легкий заработок. Вот только перед началом плодотворного сотрудничества нужно сделать взнос или сообщить данные карты, на которую доброжелатель пришлет деньги.

Типичный мошенник: обещает 15 тысяч долларов в месяц за работу, которая почти не требует усилий.

Социальному инженеру в тюрьме предстоит много интересных встреч и возможностей попрактиковаться в общении. С сокамерниками.

Коммерсант

Коммерсанты работают в сфере покупки-продажи вещей в интернете. Это не ежедневная необходимость для большинства пользователей, поэтому коммерсанты встречаются реже. Но вреда от них не меньше.

Допустим, решили вы купить зеркальный фотоаппарат. Нашли в интернете объявление: кто-то уже наигрался в фотографа и продает Canon Mark III в три раза дешевле, чем тот стоит в магазине. Вы хватаетесь за вариант: надо срочно брать, пока кто-то еще не купил. Продавец нехотя соглашается отдать камеру вам, хотя у него есть другие покупатели. Камера в соседнем городе, и завтра как раз будет okazия передать. Надо лишь отправить продавцу половину стоимости – для гарантии. Стоит ли говорить, что ни этих денег, ни камеры вы не увидите.

Более изящный сценарий: решили вы продать ноутбук. Не успели разместить объявление – звонит покупатель, готов взять, не торгуясь. Одна проблема: в ваш город он заедет только через две недели. Покупатель извиняется, что заставляет вас ждать, и хочет гарантировать сделку: просит номер карты, чтобы внести предоплату. Вы думаете: что за простофиля – отправляет деньги незнакомцу. Но простофилей будете вы, если расскажете ему данные карты.

Такие коммерсанты работают даже на популярных досках объявлений. Известность сайта вас не защитит, и лучшая стратегия – не доверять незнакомцам и никому не сообщать сведения о себе и реквизиты карты. Покупать что-то на неизвестных сайтах или форумах, где нет никаких процедур контроля и проверки продавцов, и вовсе небезопасно.

Также рискованно покупать всё, что нельзя «пощупать», например, биткоины, предметы для онлайн-игры, а также всяческие услуги «посредников», которые обещают помочь с оформлением документов, виз, справок и вида на жительство в других странах. Попытка схитрить и обмануть систему неизбежно ведет к разбитому корыту. И деньги, которые жертва добровольно отправляет мошеннику в попытке получить незаконную выгоду, не вернуть.

Всего за тысячу рублей коммерсант гарантирует гражданство США. Наверное, за пять тысяч можно стать президентом.

Не стоит доверять и сделкам через «гаранта», который якобы обеспечивает безопасность таких операций. Каким бы надежным ни казался «гарант» – насколько может казаться надежным незнакомец из интернета – есть риск, что он заберет товар, вычистит карты покупателя и продавца и пропадет.

Коммерсант знает толк в сделках. Советуем ему идти на сделку со следствием.

Внимание!

Не ходите по ссылкам, если не уверены в их надежности. Убедитесь, что отправитель – именно тот, за кого себя выдает.

Избегайте подозрительных сайтов, тем более ничего там не скачивайте.

Не сообщайте никому номер и срок действия карты, а также пароли из СМС. Сотрудник банка никогда это не спросит.

Критически подходите ко всем предложениям и объявлениям, которые встречаете в интернете. Не ведитесь на обещания халявы.

Если пришло тревожное письмо «из банка», не спешите выполнять инструкции. Позвоните в банк – но только по телефону, написанному на карте.

Не пытайтесь перехитрить других или купить что-то в несколько раз дешевле – эти мотивы ведут в руки мошенников.

Подпишитесь, чтобы получать выводы из новых статей на почту.