КАК КРАДУТ ДЕНЬГИ ЧЕРЕЗ СМАРТФОНЫ И ЧТО С ЭТИМ ДЕЛАТЬ

У четырех из пяти россиян в возрасте 16–45 лет есть смартфон. Скорее всего, у вас тоже.

Но вряд ли хотя бы один из пяти осознает, что смартфон — короткий путь к секретной информации. Через мобильные устройства злоумышленники добираются до личной переписки, банковских данных, паролей и денег.

Мобильный фишинг — новый тренд в мошенничестве. Разобраться в этой теме нам помог эксперт «Лаборатории Касперского» Виктор Чебышев, который знает о мобильных угрозах всё.

Кто в зоне риска.

Жертвой мошенников может стать каждый пользователь смартфона на Андроиде. Основная проблема Андроида в том, что на него можно поставить программу из любого источника, в том числе пиратского. С июля по сентябрь 2015 эксперты из «Лаборатории Касперского» обнаружили 320 тысяч новых мобильных вредоносных программ для этой платформы.

В зоне риска любители бесплатных игр, программ и порно. Если вы набрали в Гугле «Angry Birds скачать бесплатно» или зашли на порносайт, где вам предложили «бесплатный доступ через приложение» — вы на пороге заражения.

Немного спокойнее могут себя чувствовать владельцы айфонов. На эту платформу приходится только 0,2% вирусов и троянов. Однако это не значит, что айфоны защищены: именно ложное ощущение безопасности делает их владельцев уязвимыми. Украсть деньги можно и через айфон.

Главный фактор риска — это сам человек. Если он невнимателен, не понимает основ информационной безопасности и любит халяву, то он идеальная жертва мошенников.

Больше всех рискуют любители халявы.

Как цепляют вирусы.

Открывают ссылки из СМС. Вирусы умеют отправлять сообщения от имени реальных контактов. Вы думаете, что получили СМС от родственника и переходите по ссылке, скачиваете программу, а в ней — вирус.

СМС-вирусы стараются испугать или заинтриговать получателя, любой ценой заставляют открыть ссылку.

Не ходите по ссылкам, если не уверены в их надежности. Если ссылка пришла от знакомого, переспросите, действительно ли он отправил сообщение.

Переходят по ненадежной ссылке в интернете. Пользователи ищут интересный контент: бесплатную музыку, фильмы, игры, порно. Щелкают по ссылке, что-то скачивают, открывают, получают вирус.

После визита на торренты в загрузках возник странный файл. Не связывайтесь, пусть разбирается антивирус.

Не ищите халяву или хотя бы делайте это с компьютера. На маленьком экране смартфона сложнее распознать подозрительный сайт и выше риск нажать не туда.

Открывают файлы и зловредные ссылки в социальных сетях. Здесь люди тоже попадают в западню в поисках контента. Например, посещают сообщества с играми и переходят по ссылкам в поисках бесплатных развлечений.

Одно нажатие на иконку — и любитель поохотиться на свиней сам становится мишенью.

Устанавливайте приложения только из официального магазина: для Андроида это Google Play.

Попадают на страницы злоумышленников со взломанного сайта. Например, заходишь читать отраслевые новости на знакомый сайт, как вдруг автоматически скачивается какая-то вроде полезная программа.

Если на экране появилось непонятное приложение, открыть его — худший способ выяснить, что это такое.

Не запускайте непонятные файлы, даже если они скачались со знакомого сайта. Если что-то скачалось само, скорее всего это вирус.

Чтобы заразиться, достаточно открыть файл, полученный из ненадежного источника. После этого программа устанавливается и невидимо, в фоновом режиме выполняет всё, что в нее заложил автор.

Необходимость открыть файл — слабая защита для пользователя. Люди запускают и подтверждают всё, что угодно, — особенно когда ищут действительно интересный для них контент, например, порно. Поэтому лучше не допускать, чтобы файл с вирусом попал на смартфон.

Лучше всего использовать комплексное решение для борьбы с вредоносными программами, например, Kaspersky Internet Security для Android. Такой инструмент защищает сразу по всем фронтам: не только выявляет вирусы, но и проверяет СМС, инспектирует ссылки в браузере и загружаемые файлы, а также периодически сканирует телефон на предмет угроз.

Антивирус — это еще и единственный способ обнаружить, что телефон уже заражен, и вылечить его.

Программы, которые отправляют платные СМС

Вирус, который рассылает СМС на платные номера, — самый простой сценарий. Злоумышленнику не нужны даже банковские данные жертвы. Программа незаметно отправляет сообщения на короткий номер, и деньги со счета уходят мошеннику.

В описание некоторых СМС-вирусов авторы даже включали мелкий текст, по которому пользователь соглашался на платную подписку. Конечно, это никто не читал, но формально, получается, жертва давала согласие на списание денег.

Чтобы защитить абонентов, операторы ввели двойное подтверждение платных СМС: это когда после отправки сообщения вам приходит запрос, и вы должны подтвердить его еще одним СМС. Второе сообщение уже никак нельзя замаскировать, его должен отправить лично пользователь. Воровать деньги через платные СМС стало сложнее, и популярность этих вирусов пошла на спад.

Если пришел запрос на подтверждение платного СМС, а вы ничего не отправляли, проверьте телефон антивирусом, он может быть заражен. Если у вас стали быстро кончаться деньги на счете, посмотрите на историю списаний в личном кабинете мобильного оператора.

Не подтверждайте платные услуги, которые вы не заказывали.

Программы, которые перехватывают СМС от банка.

Когда вы покупаете что-то по карточке в интернете, банк присылает СМС с кодом подтверждения. Хакеры заражают телефоны вирусами, которые перехватывают такие коды.

К счастью, одного кода из СМС мошеннику недостаточно, чтобы украсть деньги со счета. Нужны данные карты, чтобы провести по ним платеж и подтвердить его кодом из перехваченного СМС.

Поэтому обычно сначала мошенники добывают данные карты, а потом уже заражают смартфон. Например, размещают QR-код со ссылкой на вредоносную программу и пишут, что там лежит приложение для скидок.

Вирусописатели ведут целые базы зараженных смартфонов — ботнеты. Вредоносные программы на этих устройствах дремлют на случай, если когда-то понадобятся злоумышленникам. Например, когда у мошенника есть данные карты жертвы, но нет доступа к ее телефону, он идет в ботнет. Если найдет там нужное устройство, то активирует и используют вирус.

Берегите данные карты. Когда что-то покупаете в интернете, риск нарваться на вирус выше обычного

Программы, которые маскируются под мобильный банк

Когда вы запускаете мобильный банк, зловредная программа замечает это, перехватывает управление и уводит вас к себе. После этого программа выбирает подходящее оформление и маскируется под банковское приложение. Вы не замечаете подвоха, вводите в приложении данные карты, и они утекают к мошеннику.

Банк никогда не спросит данные карты, там и так всё знают.

Помимо банков, такие программы маскируются под магазины приложений, например, Google Play. В них пользователи тоже охотно вводят данные карточки.

У пользователя три попытки понять, что перед ним вирус. На кону содержимое карты.

Число поддельных мобильных банков растет быстрее всего: в 3-м квартале 2015 в «Лаборатории Касперского» нашли в 4 раза больше таких программ, чем за предыдущие три месяца. Сейчас эксперты знают 23 тысячи программ, маскирующихся под приложения банков.

Будьте внимательны, когда открываете мобильный банк. Если видите что-то необычное при запуске или во внешнем виде приложения, это симптом. Если приложение требует лишнюю информацию, например, номер карты, бейте тревогу.

Аккуратнее с приложениями банков. Помните: банк никогда не спросит у вас данные карты или пароль.

Программы, которые используют СМС-банк.

У некоторых банков есть функция, когда командой в СМС-сообщении клиенты переводят деньги, оплачивают услуги и совершают прочие операции. Это удобно, но если телефон заражен, зловредная программа такой командой переведет деньги на интернет-кошелек или счет мобильного телефона злоумышленника.

Оцените, готовы ли держать такую брешь. Возможно, проще отключить эту услугу. Если СМС-банк вам необходим, ставьте антивирус.

Пользуетесь СМС-банком? Ставьте антивирус.

Программы, которые получают права суперпользователя

Обычно права суперпользователя — так называемый рутинг телефона — получают продвинутые пользователи, чтобы снять ограничения производителя и свободно манипулировать функциями смартфона.

К сожалению, хакеры постоянно находят уязвимости в мобильных операционных системах. В том числе такие, которые позволяют безобидным с виду приложениям сделать рутинг смартфона без ведома пользователя.

Например, вы скачиваете из магазина приложение «Фонарик». Оно не просит доступ ни к каким системным возможностям, ему даже СМС неинтересны. Но если у вас несвежая операционная система, если в ней уязвимость, то «Фонарик» сделает рутинг смартфона, а вы даже не заметите.

После этого злоумышленник получит полный доступ к устройству и всем приложениям. Он зайдет в мобильный банк и украдет оттуда номера карт и пароли.

Борьбу с такими вирусами осложняет то, что многие производители годами не обновляют программное обеспечение на своих телефонах, поэтому уязвимости, которые находят хакеры, никто не устраняет. Особенно это касается дешевых устройств.

Опасные программы встречаются даже в официальных магазинах. Чтобы снизить риск, обращайте внимание на рейтинг приложения, отзывы и количество скачиваний. И не забывайте обновлять антивирус.

Внимание!

Обновляйте антивирус и операционную систему на смартфоне.

Не ставьте странные приложения без рейтинга и отзывов.

Семь раз подумай, один раз нажми. Сомнительные ссылки — самый быстрый способ поймать вирус.

Не ищите халяву и избегайте подозрительных сайтов. Вирусописатели распространяют зловредные программы через страницы, на которых обещают бесплатный контент.

Не запускайте файлы, если не до конца в них уверены. Особенно это касается тех, что сами скачались на телефон.

Смотрите, куда приложения просят доступ при установке: фонарику не нужно уметь читать и отправлять СМС.

Обновляйте операционную систему. Назойливые исправления безопасности приходят не просто так: хакеры находят в ОС уязвимости, которые нужно устранять.

Установите надежный антивирус.

клюква
ЖИЗНЬ В САХАРЕ
Россия, 614990, Пермь, ул. Ленина, 64
телефон (342) 240–10–40
www.klookva.ru

урал фд
ПАО АКБ «Урал ФД». Генеральная лицения ЦБРФ № 249 от 12.05.2015