МОБИЛЬНОЕ МОШЕННИЧЕСТВО: ЧТО ЭТО И КАК СЕБЯ ЗАЩИТИТЬ

от компании «Лаборатория Касперского»

Мошенники постоянно придумывают новые уловки и способы обмануть нас, поэтому попытки защитить мобильные устройства уже стали частью нашей цифровой жизни. Тем не менее некоторые виды мошенничества опознать непросто, поэтому важно следить за появлением новых схем обмана и уметь их выявлять. Это гораздо эффективнее, чем восстанавливать уже украденные учетные записи.

Что такое мобильное мошенничество?

Мобильные телефоны стали для нас одним из самых ценных видов имущества, и киберпреступники об этом знают. Мы всегда носим их с собой и используем для доступа к важнейшей информации. К нашим телефонам привязаны учетные записи от банков, электронная почта и другие конфиденциальные данные, что делает их идеальной мишенью для злоумышленников.

Задача мобильного мошенника – вынудить вас самостоятельно заразить свое устройство или передать ему конфиденциальную информацию.

К самым популярным видам мобильного мошенничества относятся:

- Сообщения о заражении мобильного телефона вредоносной программой
- SMS-фишинг («смишинг»)
- Мошенничество с помощью телефонных звонков («вишинг»)
- Сбрасывающиеся звонки

Сообщения о заражении мобильного телефона вредоносной программой

При этом виде мошенничества на экране устройства отображается поддельное сообщение об обнаружении вредоносной программы.

Такое могло случаться с вами при просмотре интернет-страниц. В сообщениях обычно говорится, что в ходе сканирования на телефоне было обнаружено вредоносное ПО и вам необходимо принять срочные меры.

Вам будет предложено загрузить «антивирус», который на самом деле является вредоносной или шпионской программой. После того как вредоносный код внедрится в ваш смартфон, злоумышленники смогут получить к нему полный доступ или заразить другие устройства. Самый простой способ защититься от подобных атак – установить на свой телефон защиту, например, антивирус для устройств на Android.

Телефонный вишинг

Вишинг – это вид мошенничества, при котором вам звонят, пытаясь побудить вас к какому-либо действию.

Обычно мошенники притворяются реальными людьми или компаниями, чтобы завоевать ваше доверие. Они могут сказать, что работают в реально существующей организации, чтобы убедить вас сообщить им свои личные данные или перевести деньги.

И действий от вас ждут прямо во время телефонного разговора. Мошенники создают ощущение срочности, чтобы вы запаниковали и сделали то, чего они хотят. Вот почему они требуют заплатить или раскрыть данные прямо во время звонка, а не просят выполнить какое-то дополнительное действие позднее (после завершения разговора).

SMS-фишинг

При SMS-фишинге, или «смишинге», злоумышленники будут призывать вас к действию с помощью текстовых сообщений.

В таком сообщении может содержаться вредоносная ссылка , перейдя по которой вы загрузите на свое устройство вредоносную или шпионскую программу. Но иногда злоумышленники вынуждают жертву совершить другие действия, например, перезвонить на платный номер, оформить подписку или выдать личные данные.

Сбрасывающиеся звонки

Сбрасывающиеся звонки – это вызовы с неизвестного номера, которые длятся всего пару секунд. Это сделано для того, чтобы вынудить вас перезвонить на этот номер. Как правило, такая схема срабатывает, если ваше любопытство перевешивает критическое мышление. Хитрость в том, что обратный звонок

на подозрительный номер будет платным. На этом мошенники и зарабатывают. Обычно эти звонки совершаются с международных номеров, за что с вас и снимают деньги. Иногда мошенники оставляют сообщение в голосовой почте – это повышает шанс того, что вы решите перезвонить. Будьте осторожны, принимая звонки или прослушивая голосовую почту с неизвестного номера.

Как не попасться на мобильное мошенничество?

У каждой мошеннической схемы есть свои особенности, но, как правило, все угрозы можно разделить на несколько категорий в зависимости от целей и используемых методов. Так как новые схемы появляются регулярно, нужно быть готовым к неожиданностям и настороженно относиться к просьбам от посторонних людей. Также нелишним будет усилить защиту на своих устройствах.

Как понять, что вы столкнулись с мобильным мошенничеством?

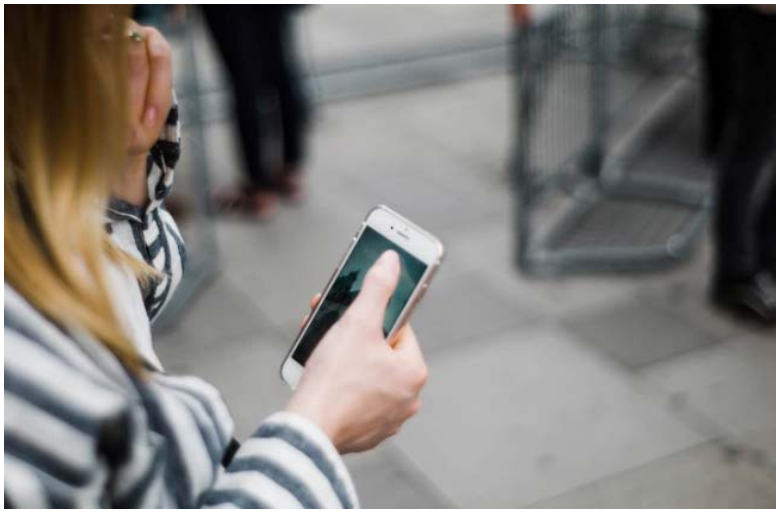
Задача любого вида мошенничества – сыграть на эмоциях и заставить вас доверять мошеннику. Вот некоторые ниточки, за которые любят дергать киберпреступники:

- ***Ощущение надвигающейся опасности подталкивает вас к активным действиям.*** Если вам кажется, что нужно срочно что-то сделать, иначе случится беда, следует остановиться и задуматься. Любой звонящий вам официальный представитель компании ответит на все ваши вопросы и подтвердит необходимость выполнения требуемого действия. Мошенники же начнут давить еще сильнее. Популярные темы мошеннических схем, где упор делается на срочность: долги, возвраты по налогам или указания на подозрение в нарушении закона.
- ***Эмпатия***, возникающая в ответ на просьбу о помощи нуждающимся. Отказаться выполнять такую просьбу сложнее. Если вы чувствуете вину за то, что сомневаетесь в реальной причине обращения к вам, это должно стать первым звонком. Мошенники могут притвориться сотрудниками благотворительной организации или придумать другую историю, а чтобы звучать более правдоподобно — упомянуть недавнюю природную катастрофу или другую актуальную проблему.
- ***Большие обещания***. Перспектива получить награду может подтолкнуть вас к выполнению просьбы мошенника. Если вы почувствовали возбуждение или надежду в отношении сделанного предложения, стоит задуматься. Например, вам могут сказать, что вы выиграли в розыгрыше или получили огромную скидку на путевку на море.

В любом случае для получения приза вас попросят что-то сделать. Вот самые популярные просьбы, к которым нужно относиться с осторожностью:

- ***Заплатить за что-либо***, особенно наличными или подарочным сертификатом. Вернуть такие платежи будет очень сложно.
- ***Выдать личную информацию***, например, номер банковского счета, номер страхового полиса или учетные данные.
- ***Перейти на сайт по ссылке***, чтобы войти в учетную запись или узнать подробную информацию.
- ***Скачать файл или приложение***, например, антивирус.

Если вам позвонили или прислали SMS с просьбой сделать что-то из вышеперечисленного, будьте осторожны. В большинстве случаев следует либо отказаться от выполнения просьбы, либо отложить ее и поискать подробную информацию.



Что делать, чтобы не попасться на мобильное мошенничество?

Лучше всего защититься от мошенников вам поможет сознательное отношение к коммуникации по телефону. Помимо умения распознавать обман вам помогут и некоторые дополнительные меры обеспечения безопасности конфиденциальных данных.

Вот несколько полезных советов для защиты от мобильного мошенничества:

При подключении к публичным сетям Wi-Fi используйте виртуальные частные сети (VPN). Шифрование в VPN-сети скроет передаваемую информацию от чужих глаз. Такие сервисы также обеспечивают анонимность, так что вас нельзя будет выследить с помощью IP-адреса или других средств. Если вы ищете сервис, который будет защищать ваши данные в интернете в пути или дома, попробуйте сервис Kaspersky Secure Connection.

Установите сложные пароли. Никогда не используйте один и тот же пароль дважды. Лучше всего создавать пароли из случайного набора знаков. Чередуйте регистр и помимо букв используйте цифры и специальные символы. Если ваш пароль – это кодовая фраза, состоящая из нескольких коротких и запоминающихся слов, замените некоторые буквы в ней символами или числами.

Используйте длинный ПИН-код. Если ваше устройство позволяет, вместо четырехзначного ПИН-кода установите на экран блокировки ПИН-код из шести знаков. Шестизначный ПИН-код образует больше возможных комбинаций, затрудняя подбор пароля злоумышленником , желающим взломать ваш телефон или учетные записи. Никогда не используйте в качестве пароля даты и другие личные данные, так как хакеры, пытаясь подобрать пароль, в первую очередь обращаются к информации, которую можно найти о вас в интернете. Также откажитесь от стандартных числовых комбинаций вроде «0000» или «1234».

Храните свои пароли в безопасном онлайн-хранилище. Чтобы не забывать свои пароли и ПИН-коды, воспользуйтесь сервисом наподобие Kaspersky Password Manager . Никогда не записывайте пароли в блокноте или в заметках на телефоне – это крайне ненадежно. Менеджеры паролей шифруют ваши данные таким образом, что взломщики не смогут их подсмотреть. Вам нужно будет запомнить всего лишь один пароль – от самого хранилища. Конечно, его нужно сделать максимально сложным и надежным, чтобы никто не смог получить туда доступ.

В настоящих розыгрышах никто не будет требовать с вас денег. Если кто-то просит вас заплатить за приз, откажитесь от затеи. Скорее всего, вы имеете дело с мошенниками.

Установите приложение, блокирующее звонки. Такие приложения защищают ваш телефон от звонков, нелегально выполняемых роботами, и прочих типов телефонного мошенничества. Однако они не всегда работают идеально и могут отправлять в спам реальные номера. К счастью, многие приложения помечают входящие звонки как потенциальный спам, позволяя вам самостоятельно решить, брать трубку или нет.

Не вступайте в разговор и положите трубку. Участие в разговоре в любом виде может спровоцировать еще больше звонков. Не нажимайте на кнопки для навигации по автоматизированному меню и не отвечайте живым операторам, если заподозрили неладное. Просто повесьте трубку и поищите в интернете информацию о звонящем, если вас все еще одолевает любопытство.

Пользуйтесь только официальными приложениями. Использование сторонних приложений для входа в такие сервисы, как онлайн-банки и социальные сети, делает ваше устройство уязвимым к несанкционированному доступу. Более того, если вы предоставите свои учетные данные сторонней организации, вы можете потерять их, оказавшись жертвой фишинга. Желательно избегать приложений, предназначенных для работы сразу с несколькими сервисами: всегда делайте выбор в пользу официальных программ.

Проверяйте телефонные счета. Если вы обнаружили в счете несанкционированные списания, вероятно, вы стали жертвой злоумышленника. Если это произошло, немедленно обратитесь к оператору и требуйте вернуть средства. Даже если причиной такого списания было не мошенничество, вы наконец отключите нежелательные услуги, накопившиеся за годы.

Установите защиту на свой телефон. Самый простой способ сохранить конфиденциальность в интернете и данные на своем телефоне – это защитить их. Мы рекомендуем воспользоваться решением Kaspersky Security Cloud, охватывающим сразу несколько устройств. Подписка Family позволит вам настраивать родительский контроль – так вы защитите себя, своего партнера и детей, если они у вас есть.

Мобильное мошенничество: что это и как себя защитить
https://www.kaspersky.ru/resource-center/threats/how-to-avoid-mobile-phone-scams