УВАЖАЕМЫЕ КЛИЕНТЫ!

В СВЯЗИ С РИСКОМ НЕСАНКЦИОНИРОВАННЫХ ОПЕРАЦИЙ (МОШЕННИЧЕСТВА), ОБРАЩАЕМ ВАШЕ ВНИМАНИЕ!

Мобильный телефон позволяет, не выходя из дома, сделать заказ в онлайн-магазине, кафе, оплатить коммунальные платежи, оформить социальное пособие или заказать справку и т. п. Но, кроме этого, телефон дает возможность мошенникам обмануть граждан.

Самая распространенная схема (на деле их гораздо больше) – когда мошенники представляются сотрудниками банка и под предлогом «подозрительных операций по вашей карте» пытаются узнать ее реквизиты и вывести денежные средства. По данным Банка России, такая технология с использованием методов социальной инженерии (когда у Вас пытаются выманить конфиденциальную информацию) стала одним из главных инструментов обмана.

ЧТО ТАКОЕ МОБИЛЬНОЕ МОШЕННИЧЕСТВО?

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

К самым популярным видам мобильного мошенничества относятся:

1) 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 программное обеспечение 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.

2) 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 (например, в службе безопасности Банка), чтобы убедить вас сообщить им свои личные данные или перевести деньги.

С помощью специальных сервисов IP-телефонии злоумышленники могут подменять номер, который будет выглядеть как номер Вашего банка.

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 (перевести деньги) или раскрыть данные прямо ***во время звонка***, а не просят выполнить какое-то дополнительное действие позднее (после завершения разговора).

3) SMS-фишинг.

При SMS-фишинге 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.

4) 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?

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:

1) 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.

2) Установите приложение, блокирующее звонки. Такие приложения защищают ваш телефон от звонков, нелегально выполняемых роботами, и прочих типов телефонного мошенничества.

3) 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.

4) 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.

5) 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.

6) 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.

7) 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. Также откажитесь от стандартных числовых комбинаций вроде «0000» или «1234».

8) Пользуйтесь только официальными приложениями из магазинов App Store, Google Play, Microsoft Store. Никогда не пользуйтесь другими неофициальными приложениями во избежание передачи личной информации мошенникам.

9) Установите защиту на свой телефон. Самый простой способ сохранить конфиденциальность в интернете и данные на своем телефоне – это защитить их. Владельцам смартфонов настоятельно рекомендуем использовать антивирусное программное обеспечение, которое поможет уменьшить вероятность попадания в устройство вредоносных программ, предназначенных для перехвата приходящих от банка СМС-сообщений, кражи персональных данных и авторизационных данных карты.

КУДА ОБРАЩАТЬСЯ В СЛУЧАЕ МОШЕННИЧЕСТВА

Если Вы получили подозрительное письмо, звонок или обнаружили операцию, которую Вы не совершали, а также в случае, когда доступ к вашему компьютеру, смартфону или USB-токену могли получить посторонние лица, немедленно обратитесь в Банк по телефону +7 (3952) 24-16-02 или +7 (3952) 24-01-12.

ВНИМАНИЕ!

Незамедлительное обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств со счетов может позволить оперативно приостановить транзакцию и предотвратить финансовые потери.