РЕКОМЕНДАЦИИ: КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ В МЕССЕНДЖЕРАХ?

67% граждан России за последний год получали звонки от мошенников, но почти половина опрошенных считает, что обмануть их вряд ли получится, а еще 27 % полагают, что это вообще невозможно. Однако, с 2022 года по август 2024 года в России произошло около 1,5 миллионов киберпреступлений, а за последние 3 года мошенники похитили у россиян и вывели за границу более 350 миллиардов рублей. Злоумышленники продолжают придумывать новые схемы обмана и с развитием технологий стратегии становятся все более изощренными.

1 Просьба проголосовать за знакомого, участвующего в конкурсе

Как правило Вы получаете от знакомого ссылку с просьбой проголосовать в каком-то конкурсе. Это одна из самых распространенных схем, как правило, речь идет о конкурсе, в котором принимает участие ребенок или иной близкий родственник. Это естественная просьба, типичная для общения в соцсетях и мессенджерах, которая не вызывает подозрений. Кроме того, это не просьба одолжить денег, так что уровень бдительности сразу снижается. У пользователя не возникает ощущения, что он сейчас чем-то рискует.

После того, как Вы переходите по ссылке, мошенники получают доступ к Вашему аккаунту и рассылают аналогичную просьбу Вашим контактам, а некоторые из знакомых получают сообщение с предложением перевести деньги на банковскую карту. Это цепочка взломов, причем первые взломы содержали только просьбу проголосовать и перейти на некий сайт, а позднее уже начинают приходить просьбы о перечислении денег.

Как защититься:

- ✓ **Будьте внимательны к неожиданным просьбам от знакомых и свяжитесь с тем, кто просит о помощи по телефону;**
- ✓ **Не переходите по незнакомым ссылкам.** Если кто-то предлагает Вам сайт, где нужно ввести пароль от вашего профиля, не торопитесь и проверьте, действительно ли этот ресурс связан с тем, о чем говорит собеседник;
- ✓ **Не делитесь личной информацией**. Не вводите свои личные данные (номер телефона, код подтверждения, пароль) на страницах, которые не являются официальными ресурсами мессенджера;
- ✓ **Не поддавайтесь панике и не принимайте поспешных решений**.

2 Важные сообщения от «руководителя»

Мошенник представляется Вашим начальником и просит выполнять его задания. Сценариев сотни, сюжетных линий - десятки. «Начальник» обращается к Вам со срочной просьбой, которую необходимо выполнить немедленно, иначе компания, в которой Вы работаете, столкнется с рядом «серьезных проблем».

1.) Мошенники создают в мессенджерах поддельные аккаунты: с реальной фотографией и ФИО руководителя (директора компании, главврача больницы, ректора учебного заведения и т.п.) либо непосредственно взламывают мессенджер руководителя. С этого аккаунта пишут сотруднику организации.

2.) Фейковый руководитель сообщает, что скоро этому сотруднику должны позвонить из уполномоченного органа по очень важному вопросу. Подчеркивается, что подчиненный должен следовать инструкциям, полученным по телефону, и не сообщать никому об этом разговоре.

3.) Подготовленный к будущей беседе с «представителем власти» сотрудник теряет бдительность, и, не желая быть уволенным, выполняет все, что ему скажут.

4.) Цель таких звонков – заставить жертву перевести деньги на «безопасный счет», а также собрать сведения, которые будут использовать для дальнейших атак, о других сотрудниках или компании.

Как защититься:

- ✓ **Свяжитесь с тем, от чьего имени исходит просьба либо уточните информацию у своих коллег.** Злоумышленники обычно торопят и запрещают кому-либо рассказывать о разговоре. Возьмите паузу, сообщите о подозрительных звонках своему руководителю и обсудите с ним ситуацию;
- ✓ **Не поддавайтесь панике и не принимайте поспешных решений;**
- ✓ **Помните, что никто не вправе давать Вам какие-либо поручения о переводе денежных средств;**
- ✓ **Если Вы поняли, что перед Вами мошенник - заблокируйте его аккаунт в приложении, а также предупредите коллег о появлении таких профилей и номеров.**

3 Фальшивые уведомления

Вам может прийти сообщение или уведомление от якобы известного банка, почтовой службы или от администрации мессенджера. В нем будет уведомление о проблеме с аккаунтом или оплатой, и предложение срочно перейти по ссылке для решения вопроса. На самом деле это ловушка, которая перенаправит на поддельный сайт.

Как защититься:

- ✓ **не переходите по ссылкам из подозрительных сообщений**. Если сомневаетесь, то позвоните в компанию или посетите ее официальный сайт напрямую.

4 Как повысить защищенность своего аккаунта

Telegram

✓ **Включите двухфакторную аутентификацию**

— Инструкция для Android: откройте раздел «Настройки» → «Конфиденциальность», выберите опцию «Двухэтапная аутентификация» и включите ее. После этого остается только придумать пароль и нажать «Готово». При наличии PIN-кода, привязанного к устройству, мошенник не сможет получить доступ к профилю, даже если перехватит SMS-сообщение с секретным кодом

— Инструкция для iOS: откройте раздел «Настройки» → «Конфиденциальность» и выберите опцию «Облачный пароль». Далее точно так же нужно придумать пароль и нажать «Готово».

✓ **Настройки конфиденциальности**

Откройте раздел «Настройки» → «Конфиденциальность», в данном разделе можно установить видимость своих личных данных (телефон и т.д.) только для Контактов. Также ограничить возможность звонить Вам через Telegram и приглашать Вас в группы и каналы.

✓ **Контроль связанных устройств**

Регулярно проверяйте связанные устройства. «Настройки» → «Устройства» → «Завершить все другие сеансы».

WhatsApp

✓ **Включите двухфакторную аутентификацию**

«Настройки» → «Аккаунт» → «Двухшаговая проверка». После этого остается только придумать пароль и нажать «Готово». При наличии PIN-кода, привязанного к устройству, мошенник не сможет получить доступ к профилю, даже если перехватит SMS-сообщение с секретным кодом.

✓ **Настройки конфиденциальности**

«Настройки» → «Аккаунт» → «Конфиденциальность» → «Видимость персональных данных». Нужно разрешить просмотр личной информации только Вашим контактам. В том же меню ниже рекомендуется запретить добавление Вас в группы незнакомцами. При этом у человека все равно будет возможность пригласить вас в общий чат, но это будет сделано не автоматически, а по предварительному запросу, который всегда можно отклонить.

✓ **Контроль связанных устройств**

Регулярно проверяйте связанные устройства. Перейдите в «Настройки» → «Связанные устройства», чтобы просмотреть все устройства, связанные с вашим аккаунтом WhatsApp. Чтобы удалить связанное устройство, нажмите «Выйти».

Viber

✓ **Включите двухфакторную аутентификацию**.

«Еще» → «Настройки» → «Конфиденциальность» → «Двухэтапная проверка». После этого остается только придумать пароль и нажать «Готово». При наличии PIN-кода, привязанного к устройству, мошенник не сможет получить доступ к профилю, даже если перехватит SMS-сообщение с секретным кодом.

✓ **Настройки конфиденциальности**

«Еще» → «Настройки» → «Конфиденциальность». В данном разделе, можно установить флажки в подразделах:

— Настройка добавления в группы (выбрать «Мои контакты»);

— Верифицировать контакты (верификация - проверка пользователя на достоверность внесенных данных);

— Автопроверка на спам.

Также можно отключить рекламную рассылку в разделе: «Еще» → «Настройки» → «Конфиденциальность» → «Личные данные».

✓ **Защита от лишних звонков**

«Еще» → «Настройки» → «Вызовы и сообщения». В данном разделе выставить флажок в графе «Защита от лишних звонков»

✓ **Контроль связанных устройств**

«Еще» → «Настройки» → «Учетная запись» → «Компьютеры и планшеты». В данном разделе можно деактивировать доступ на других ранее подключенных Ваших устройствах (к примеру, на компьютере). Деактивация не лишит вас возможности вновь активировать аккаунт на данных устройствах.

Порядок действий, если Вы все-таки стали жертвой мошенников

✓ Обратиться на горячую линию своего банка (в случаях, когда мошенникам получили доступ к денежным средствам на Вашей банковской карте). Дополнительно подать заявление об ошибочности платежа и подробно описать ситуацию.

✓ Обратиться в службу поддержки мессенджера для блокировки своего аккаунта (в случаях, когда злоумышленники получили доступ к Вашему аккаунту). Попытаться самостоятельно произвести блокировку.

✓ Сообщить как можно быстрее в правоохранительные органы о случае мошенничества и максимально подробно описать свою ситуацию.

✓ Поставить в известность близких родственников.