Адкрытае акцыянернае таварыства
«Торфабрыкетны завод Лідскі»

Открытое акционерное общество
«Торфобрикетный завод Лидский»

З А Г А Д

П Р И К А З

30.12. 2022 № 338

п. Первомайский Лидского р-на
Гродненской обл.

О проведении профилактической работы

На основании письма Следственного комитета Республики Беларусь от 23.12.2022№10-29/2485-14 «О проведении профилактической работы» и во исполнение Закона Республики Беларусь от 04.01.2014 №122-З «Об основах профилактики правонарушений»,

ПРИКАЗЫВАЮ:

1. Руководителям структурных подразделений под персональную ответственность довести до сведения подчиненных работников Памятку Следственного комитета о профилактике по неправомерному завладению реквизитами, личными данными и последующего хищения средств с карт счетов граждан (далее –Памятка) на собраниях трудового коллектива с оформлением протокола, а ответственному за ведение идеологической работы Белан Л.В. – до административно-управленческого персонала.

Срок проведения – до 10.01.2023

2. Белан Л.В., ответственной по работе со СМИ и общественностью разместить на сайте предприятия и на информационном стенде Памятку.

Срок проведения – до 09.01.2023

3. Контроль за исполнением приказа возложить на Белан Л.В., ответственного за ведение идеологической работы.

Директор И.П.Залеский

Юрисконсульт
И.А.Аксёненко
30.12.2022

Иногда аккаунты Viber взламывают для создания бота для рассылки спама всем доступным контактам.

Если с вами это случилось, то не расстраивайтесь, ведь есть несколько проверенных способов спасения своего аккаунта или хотя бы своей личности в глазах друзей.

Далее мы поговорим о таких способах спасения и о действиях, которые помогут вам спасти аккаунт в дальнейшем.

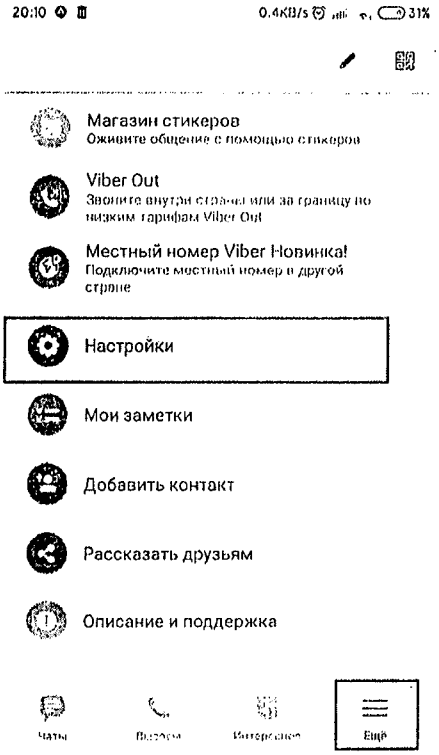
УДАЛЕНИЕ ВСЕХ ПОДОЗРИТЕЛЬНЫХ УСТРОЙСТВ

Если кто-то входит в ваш аккаунт без вашего разрешения, но у вас есть доступ к аккаунту на вашем мобильном устройстве, то можно скинуть с аккаунта другие устройства взломщика. Для этого последуйте следующей инструкции:

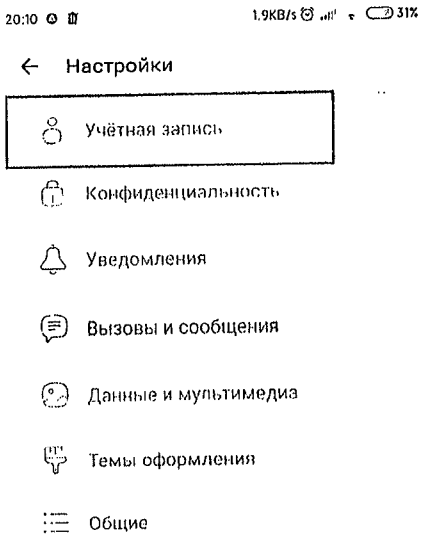
Откройте приложение через мобильное устройство

Снизу найдите и откройте вкладку «Еще»;

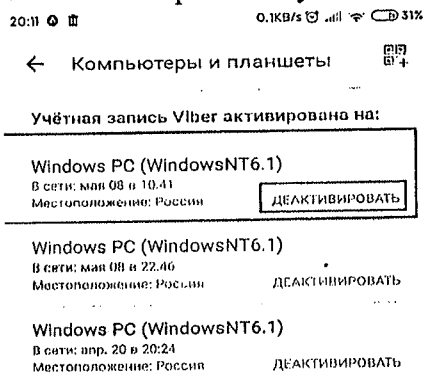
Среди пунктов меню найдите «Настройки»;



В открывшимся меню найдите пункт «Учетная запись»;



Уже в настройках учетной записи найдите пункт «Компьютеры и планшеты»;



Откроется список из всех устройств, на которых прямо сейчас, в момент открытия установлен Viber и был совершен вход на ваш аккаунт.

П осле удаления приложения устройство автоматически деактивируется, так что среди них может быть устройство взломщика, через которое он прямо сейчас управляет вашим аккаунтом.

Найдите и деактивируйте все подозрительные устройства, обращайте особое внимание на устройства на базе IOS или Windows;

После деактивации устройств, проделайте действия по защите аккаунта.

СООБЩЕНИЕ В СЛУЖБУ ПОДДЕРЖКИ

Напишите в службу поддержки и опишите всю достоверную информацию о аккаунте, обязательно введите правильные почту – туда будет отправлен ответ и номер телефона, к которому привязывался аккаунт.

Служба поддержки, в случае если других вопросов у нее не будет, обязательно вам поможет и посодействует в безопасном спасении аккаунта от злоумышленника.

РАДИКАЛЬНАЯ МЕРА – УДАЛЕНИЕ АККАУНТА

Если даже служба поддержки вам не помогла или вы не знаете, какие устройства ваши, то лучше полностью удалить свой аккаунт.

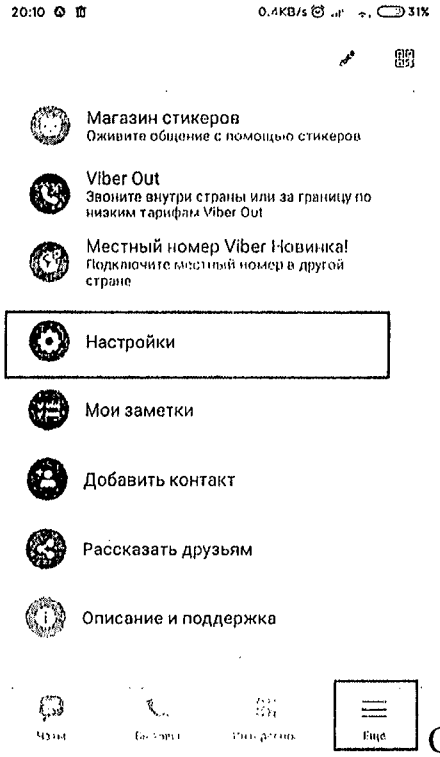
Удаление аккаунта – радикальный способ решения проблемы, который влечет несколько минусов за собой:

Все ваши переписки, файлы и другая информация о вашем аккаунте пропадет без возможности восстановления.

Вы сами пропадете из чатов своих друзей. Лучше всего сохранить всю важную информацию перед этим делом.

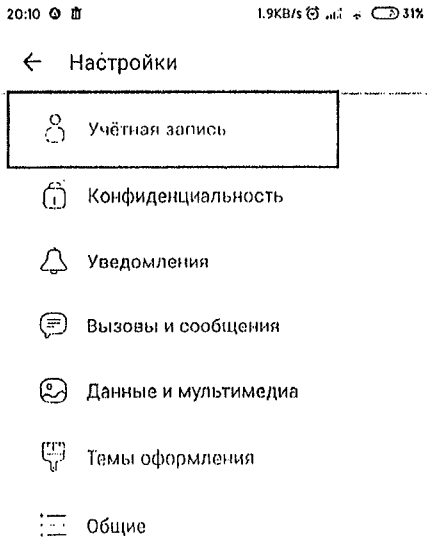
Вы совершите выход со всех своих устройств: компьютера, планшета и других, на которых был совершен вход.

Е сли терять на аккаунте вам уже нечего, проделайте следующие действия.

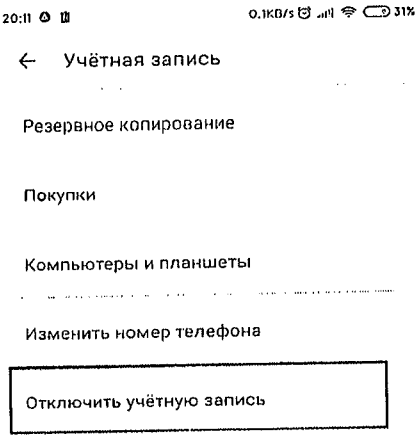


Откройте вкладку «Еще»;

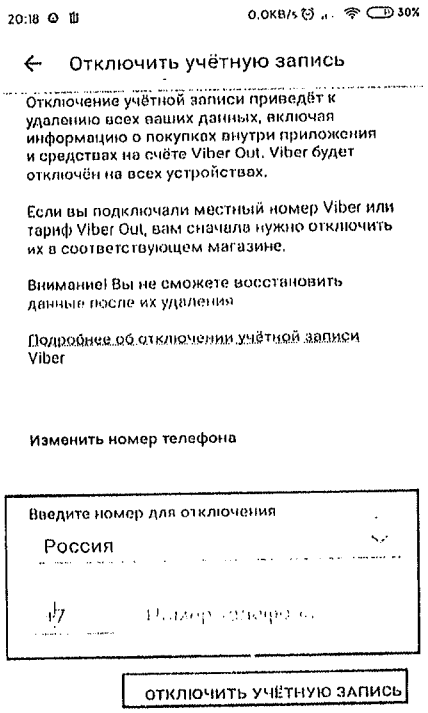
Откройте настройки;



Найдите пункт «Учетная запись»;



Нажмите «отключить учетную запись»;



Правильно введите и подтвердите свой номер телефона. Удалите учетную запись;

Проделайте все меры защиты своего аккаунта от взлома.

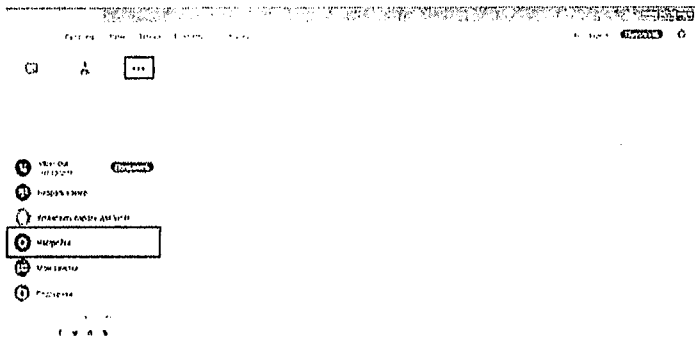
СПОСОБЫ ЗАЩИТЫ АККАУНТА

Если ваш аккаунт взломали, и вам удалось отбить его у злоумышленника, или вы просто хотите защитить свой аккаунт от малейших попыток кражи, то вам помогут следующие способы защиты аккаунта.

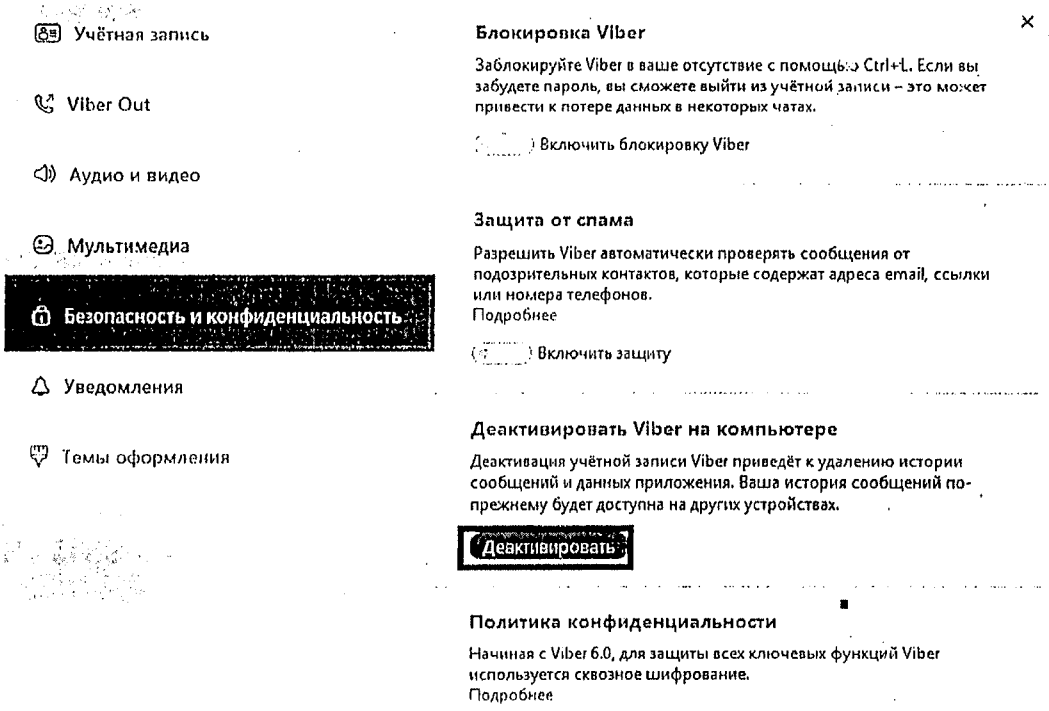
НИКОГДА не сообщайте числовые пароли из SMS сообщений, даже близким людям, возможно их тоже могли взломать;

Удалите все подозрительные приложения из телефона, скачайте антивирус, не скачивайте ПО из непроверенных источников и никогда не давайте подозрительным программам доступ к своим SMS сообщениям;

После каждой работы за чужим компьютером в Вайбере, проделайте следующие действия:



Зайдите во вкладку дополнительного меню;
Откройте настройки;
Выберете вкладку «Безопасность и конфиденциальность»;



Нажмите «деактивировать».

Мошенники стали использовать новую схему в Telegram, предлагая пользователям подарок - премиум доступ к услуге по ссылке. На деле же переход по ссылке может обернуться кражей личных данных.

Мошенники стали использовать новую схему в Telegram, предлагая пользователям подарок - премиум доступ к услуге по ссылке. На деле же переход по ссылке может обернуться кражей личных данных.

Схема следующая. Пользователь получает ссылку на «подарок» - якобы бесплатный доступ к премиум-аккаунту Telegram. Для получения премиума необходимо всего лишь перейти по ссылке. Ссылка приходит от пользователя, которого взломали. После того, как пользователь перешел по ссылке, приходит код авторизации. На экране с подарком написано, что этот код необходимо ввести, чтобы активировать премиум-подписку. После введения пользователем этого кода его аккаунт открывается у мошенника на компьютере. Новый аккаунт сразу же рассылает подобные сообщения по всему списку контактов и удаляет их из списка отправленных.

Если **Вы перешли по такой ссылке**, то необходимо:

Зайти в настойки Telegram.

Выбрать "Устройства", "Активные сеансы".

Просмотреть устройства, с которых заходили в Ваш аккаунт. Если есть не Ваши устройства, то на них необходимо завершить сессию и сменить пароль, если он был установлен.

Если не была включена двухфакторная аутентификация - обязательно включить.

Рекомендуется установить код-пароль для входа в Telegram.

Обращаем внимание, что такая схема несанкционированного доступа к аккаунту не сработает, если была подключена двухфакторная аутентификация.

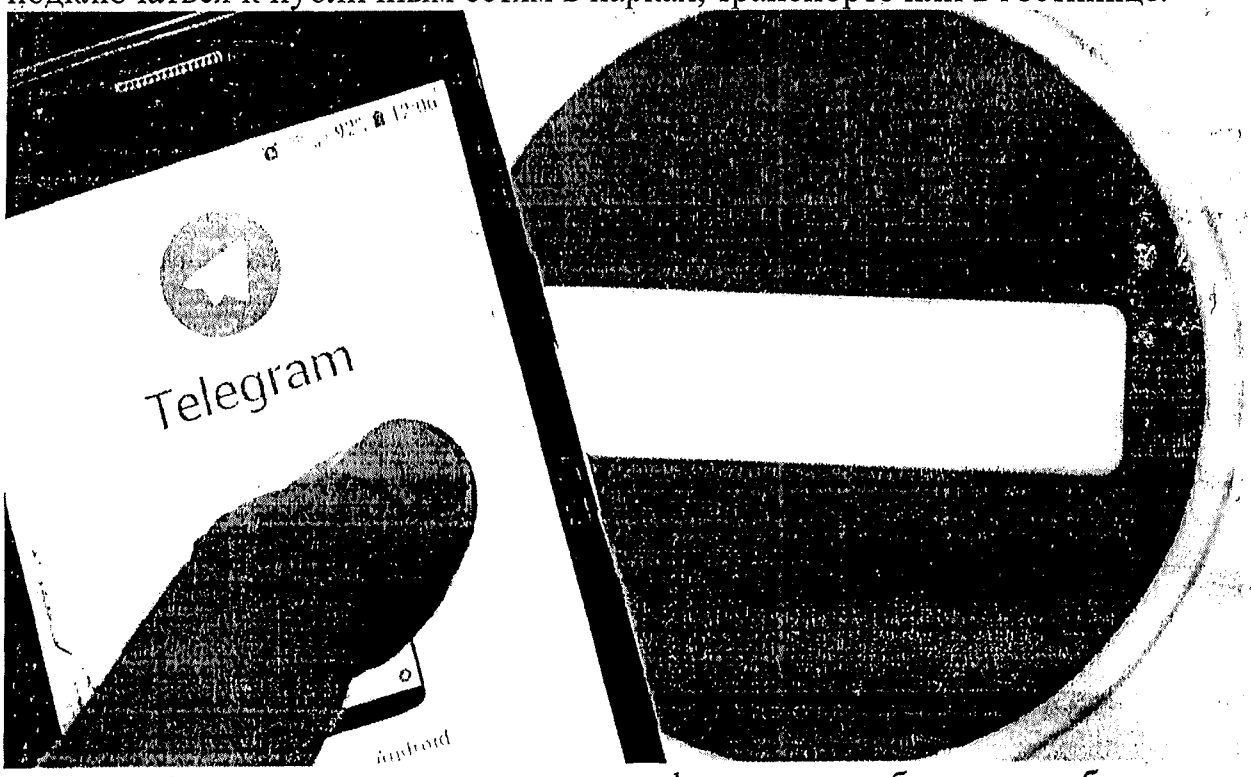
Говоря о мошенничестве через мессенджеры, важно понимать, что Telegram - это всего лишь способ связи. Суть схем не меняется - происходит то же самое, что в соцсетях и по телефону.

1. Мошенники выводят жертву на диалог. Для этого они притворяются знакомыми или доверенными каналами, маскируются под рекламу (а порой дают реальные рекламные объявления) или звонят в обход антифрод-защиты операторов. Следующий шаг - отправка фишинговой ссылки либо незатейливая просьба перевести деньги прямо на счет.

2. Кража аккаунта. В этом случае может использоваться, например, сценарий с просьбой проголосовать за работу ребенка на конкурсе рисунков. Чтобы оставить свой голос, нужно ввести свои данные в фишинговой форме и указать код авторизации в мессенджере.

Такой тип преступлений особенно характерен для Telegram, который давно перестал быть просто мессенджером и превратился, по сути, в социальную сеть, где существуют каналы с сотнями тысяч и даже миллионами подписчиков.

Взломать Telegram гораздо проще, если устройства преступника и жертвы находятся, например, в одной Wi-Fi-сети, поэтому не стоит подключаться к публичным сетям в парках, транспорте или в гостинице.



Чтобы не попасться на крючок аферистов необходимо соблюдать в Telegram определенные меры безопасности:

Для минимизации возможных рисков следует использовать сложные пароли и дополнительные средства защиты Вашего аккаунта, такие как двухфакторная аутентификация (облачный пароль).

При малейших сомнениях рекомендуется проверять присланные файлы или архивы на наличие угроз. Важно установить защитное решение на тех устройствах, на которых это возможно.

Если появились подозрения, обратите внимание на раздел «Активные сеансы»: при обнаружении неизвестного или подозрительного устройства завершите эту сессию и смените установленный пароль.