МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ
УВД МОГИЛЕВСКОГО ОБЛАСТНОГО ИСПОЛНИТЕЛЬНОГО КОМИТЕТА
КРИМИНАЛЬНАЯ МИЛИЦИЯ
УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙТСВИЮ КИБЕРПРЕСТУПНОСТИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по минимизации негативных последствий в части возможных угроз, осуществляемых посредством использования интернет- мессенджеров

МОГИЛЕВ,2024

1. **Как защитить свой аккаунт в Telegram** **стр.3**
2. **Как защитить свой аккаунт в Viber** **стр.6**
3. **Как защитить свой аккаунт в WhatsApp** **стр.8**

1. Как защитить свой аккаунт в Telegram

Telegram хорошо защищенный мессенджер, но не все настройки приватности и защиты активированы по умолчанию.

Чтобы аккаунт был под максимальной защитой просмотрите на следующие настройки:

1. Двухфакторная авторизация

Важнейшая защита вашего аккаунта. Если не установлен пароль Вы можете лишиться своего профиля путем перехвата смс при авторизации, с помощью дублирования sim-карты, действия спецслужб через работников мобильных операторов. Двухфакторная авторизация включается по следующему пути: **Настройки – Конфиденциальность – Двухэтапная аутентификация.**

После ввода пароля будет предложено указать электронную почту, через которую можно будет восстановить забытый пароль. Если ее не указать, а потом забыть пароль, восстановить доступ к аккаунту будет непросто: что делать, если забыл облачный пароль.

Максимальную защиту даёт пароль без указания электронной почты. Так возможность взлома аккаунта будет сведена к минимуму, но появится шанс забыть или потерять пароль, что приведёт к полной утрате аккаунта без возможности его восстановления, об этом подробнее в отдельной статье.

2. Код пароль

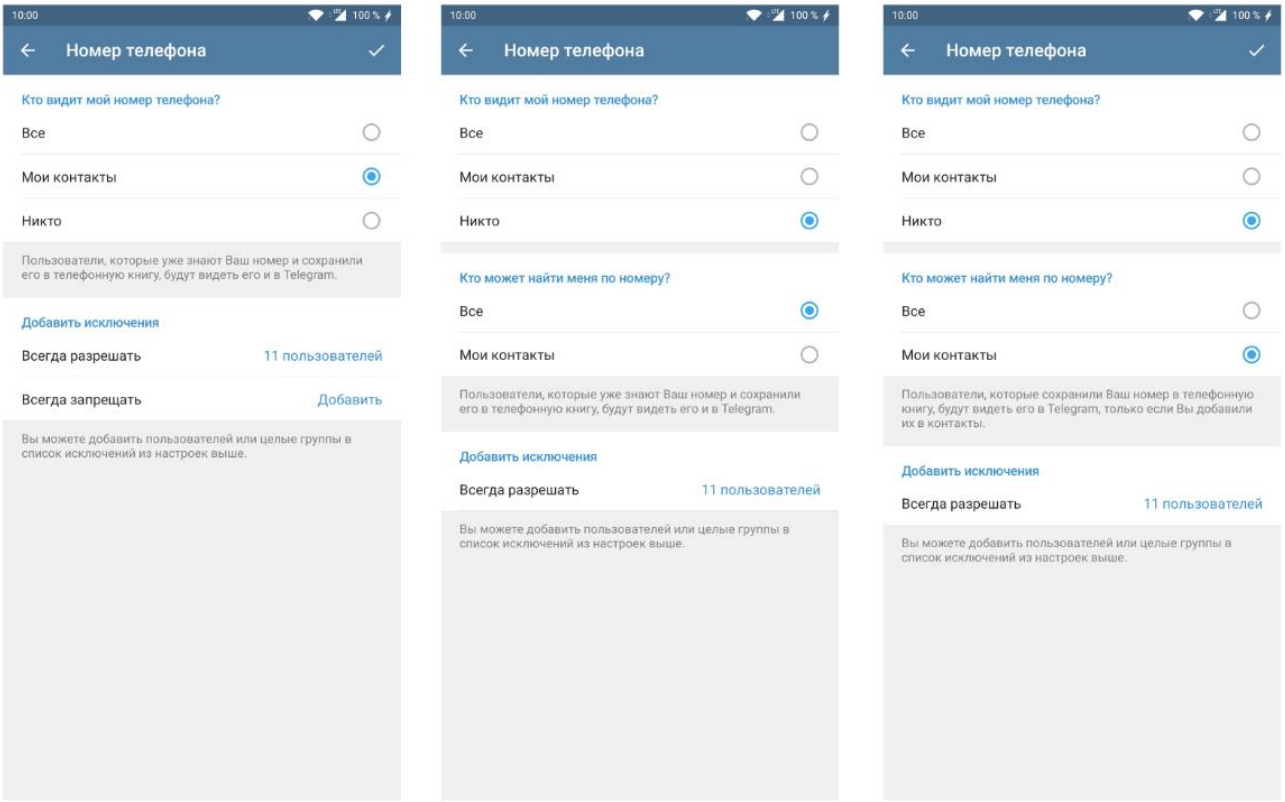
Настройки – Конфиденциальность – Код-пароль

Дополнительная защита вашего приложения – это код на него похожий на тот, который ставится на само ваше устройство. Можно выбрать разблокировку по отпечатку пальца или Face ID, или только код. Можно поставить автоблокировку через определенный промежуток времени, или блокировать приложение вручную. Такая защита во многом дублирует защиту Вашего мобильного устройства и часто избыточна, но она может понадобиться, если Вы не ставите пароль на доступ к телефону или компьютеру.

3. Видимость номера

В Telegram, как и в других мессенджерах существует возможность импорта контактов для проверки, зарегистрирован ли аккаунт на конкретный номер, таким образом недобросовестные личности или организации могут создавать базы пользователей Telegram. Так недавно утекла база 40 млн. пользователей Telegram. Для проверки, попал ли Ваш номер в эту базу можно воспользоваться ботом t.me/infoleakbot, он не получает никаких Ваших данных за исключением Вашего ID и проверяет Вас по слитой базе.

Скрыть свой номер важно как для тех, кто нашёл себя в подобных базах, так и для тех, кто не хочет в будущем увидеть себя в них.



Настройки – Конфиденциальность – Номер телефона

По умолчанию в Telegram стоит пункт **Мои контакты** и Ваш номер будет виден только тем, у кого был Ваш номер и те, чей номер есть у Вас.

Поставив галочку, **никто**Вы запрещаете видеть Ваш номер тем, кто записан у Вас в записной книжке, но не имеет Вашего номера телефона, а также открываете еще одно меню:

4. Кто может найти меня по номеру

Выбрав вариант **Мои контакты,**Вы скроете от неизвестных Вам людей свой профиль. Занеся Вас в телефонную книгу, Telegam попросту не покажет ищущему, что Ваш профиль есть в мессенджере. Такая настройка может затруднить поиск Вашего контакта в Telegram тем, кого Вы не добавили в записную книжку.Решите для себя, что Вам важнее: приватность или открытость для новых людей.

5. Запретить отображение аватарки и профилей при пересылке сообщений

Вы можете скрыть свою аватарку от незнакомых пользователей и запретить переходить к Вашему профилю через пересланные от Вас сообщения. Кроме этого, Вы можете изменить своё реальное имя на псевдоним – это подойдёт тем, кто старается соблюдать максимальную конфиденциальность в мессенджере. Не используйте юзернейм, который установлен у вас в других соцсетях, фамилию или адрес почты. Так Вас будет просто вычислить.

Настройки конфиденциальности искать тут:

Настройки – Конфиденциальность – Фото на аватаре

Настройки – Конфиденциальность – Профиль при пересылке

6. Запрет на звонки и приглашения в группы

Если Вы не хотите раскрывать свою личность, обязательно отключите возможность звонить Вам. Так Вы можете скомпроментировать себя, особенно если случайно ответите на видеозвонок. Искать здесь:

Настройки – Конфиденциальность – Звонки – Никто

Настройки – Конфиденциальность – Группы – Мои контакты

2. Как защитить свой аккаунт в Viber

1.Настройки конфиденциальности

Используйте меню настроек и особенно настройки конфиденциальности, чтобы управлять различными аспектами конфиденциальности в приложении. Здесь Вы найдете такие важные функции, как Скрытые чаты, настройки персональных данных, запросы на переписку, верифицированные контакты и т.д.

Нажмите: ещё> Настройки> Конфиденциальность.

2.Кто может добавлять вас в группы?

Иногда знакомые или коллеги могут добавлять Вас в интересные для них групповые чаты в Viber. Теперь Вы сами можете решать, кто может добавлять вас в группы: кто угодно или только контакты из вашей адресной книги. Сделать это проще простого:

Настройки> Конфиденциальность> Настройки добавления в группы.

3.Блокировка экрана Viber на компьютере

Иногда одним компьютером пользуются несколько человек, но это не значит, что Вы должны делиться с ними своей учетной записью в Viber.

В Viber для компьютера Вы можете ввести пароль и заблокировать окно приложения, чтобы никто не прочитал Ваши чаты.

Нажмите: ещё> Установить пароль для Viber.

4.Настройка статусов “В сети” и “Просмотрено”

Не хотите, чтобы другие пользователи знали, прочитали ли Вы их сообщения, и когда Вы в последний раз были онлайн? Нет проблем. Просто отключите эти статусы в настройках конфиденциальности.

Нажмите: ещё> Настройки> Конфиденциальность> отключите статус “В сети” / “Просмотрено”.

5.Скрытые чаты

Некоторые чаты особенно важны и требуют дополнительного уровня безопасности. Для таких случаев используйте скрытые чаты. Они хранятся отдельно от обычных чатов и доступ к ним можно получить, введя PIN-код.

Нажмите: ещё> Настройки> Конфиденциальность> Скрытые чаты.

6.Защита данных

Личные данные должны оставаться личными, поэтому Вас никогда не попросят предоставить их в чате Viber.

Официальные сообщения от Viber всегда приходят на официальный чат, который имеет значок верификации синего цвета.

Viber никогда не запрашивает в чате Ваши персональные данные, включая информацию о банковских картах и/или коды подтверждения.

7.Проверка на спам

Иногда Вы можете получать от неизвестных пользователей сообщения, которые могут причинить вред, если содержат ссылки, номера телефонов или email. Чтобы защитить Вас от неприятных последствий, в Viber Вы можете включить автоматическую проверку сообщений на спам. Viber проверит сообщения от неизвестных пользователей и даст Вам знать, безопасно ли открывать их.

В Viber для компьютера кликните: Ещё > Настройки > Безопасность и конфиденциальность > включите защиту от спама.

8.Вход с помощью пароля.

Ваша учетная запись будет в безопасности, если Вы включите 6-значный пароль, который нужно вводить при регистрации нового устройства в Viber. Активировав эту функцию, Вы всегда будете уверены, что никто не сможет добавить новое устройство к Вашей учетной записи без вашего ведома.

Нажмите: Настройки > Конфиденциальность > Защита паролем.

9. «Защита от лишних звонков» в Viber

В мобильном приложении:

перейдите в раздел **«Ещё»**>откройте вкладку **«Настройки»>**выберите **«Вызовы и сообщения»>**установите галочку на пункте **«Защита от лишних звонков».**

На веб-версии:

перейдите в раздел **«Ещё»>** откройте вкладку **«Настройки»>** выберите **«Безопасность и конфиденциальность»>** переведите тумблер на включение в пункте **«Защита от лишних звонков».**

После этого Вы не будете получать входящие видео- и аудиозвонки от неизвестных контактов. Информация об этих звонках будет сохранена только в списке чатов как «Пропущенный вызов», а также в разделе «Недавние вызовы».Так Вы не пропустите ничего важного и сможете перезвонить при необходимости.

3. Как защитить свой аккаунт в WhatsApp

Ни в коем случае не делитесь своим кодом регистрации и PIN-кодом двухшаговой проверки с другими.

Включите двухшаговую проверку и укажите свой адрес электронной почты – он поможет Вам восстановить доступ к аккаунту, если Вы забудете свой PIN-код.

Чтобы включить двухшаговую проверку:

1. Откройте **Настройки WhatsApp**> Нажмите **Аккаунт / Учётная запись** >**Двухшаговая проверка**>**Включить**.
2. Введите желаемый шестизначный PIN-код и подтвердите его.
3. Укажите адрес электронной почты, к которому у Вас есть доступ, или нажмите **Пропустить**, если не хотите указывать адрес. Рекомендуется указать адрес электронной почты, так как это поможет защитить Ваш аккаунт и позволит сбросить двухшаговую проверку в случае необходимости.
4. Нажмите **Далее**.
5. Подтвердите адрес электронной почты и нажмите **сохранить** или **Готово**.

Если Вы забыли PIN-код и при этом не указали свой адрес электронной почты, Вы сможете сбросить PIN-код только через 7 дней. Поскольку не осуществляется проверка, правильно ли Вы указали адрес электронной почты, удостоверьтесь, что его написание верно и что у Вас есть к нему доступ.

Чтобы изменить PIN-код двухшаговой проверки:

Откройте **Настройки WhatsApp**>Нажмите **Аккаунт / Учётная запись**>**Двухшаговая проверка**>**Изменить PIN**.

Чтобы добавить адрес электронной почты:

Откройте **Настройки WhatsApp**> Нажмите **Аккаунт / Учётная запись**>**Двухшаговая проверка**> нажмите **Добавить адрес эл. почты**.

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

Установите код устройства. Будьте осторожны, предоставляя кому-либо физический доступ к вашему телефону. Имея физический доступ к устройству, человек может воспользоваться Вашим аккаунтом WhatsApp без вашего ведома.

Мы рекомендуем Вам поделиться этими советами с родственниками и друзьями, чтобы их аккаунты WhatsApp также были защищены наилучшим образом.

Если Вы получите электронное письмо для сброса PIN-кода двухшаговой проверки или кода регистрации, но Вы его не запрашивали, не нажимайте на ссылку. Возможно, кто-то пытается получить доступ к вашему номеру телефона в WhatsApp.

УПК КМ УВД Могилевского облисполкома