**Главное управление по противодействию киберпреступности криминальной милиции МВД РеспубликиБеларусь**

# ЗАЩИТА ОТ МОШЕННИКОВ

## Настройка смартфона и мессенджеров

### Комплект памяток для граждан и тех, кто помогает настроить телефон

Telegram • WhatsApp • Viber • Android • iPhone

**Самая важная мысль**

Ни одна настройка не даёт полной защиты. Главная защита: положить трубку, ничего не сообщать и самостоятельно перезвонить близкому человеку, банку или организации по сохранённому официальному номеру.

**При совершении мошенничества немедленно звоните в милицию по номеру 102.**

## Как использовать комплект

- Страница 2 предназначена владельцу телефона: её лучше распечатать и положить рядом с телефоном.
- Страницы 3–7 предназначены помощнику, который один раз настраивает телефон и проверяет результат.
- Страницы 8–9 нужны на случай подозрительного контакта или уже совершённой ошибки.

## Выберите режим защиты

| **ОБЫЧНЫЙ РЕЖИМ**<br>Рекомендуется большинству | **МАКСИМАЛЬНЫЙ РЕЖИМ**<br>Для человека, которому почти никто новый не звонит |
|---|---|
| В мессенджерах звонят только контакты. Обычный телефон показывает и фильтрует спам. Незнакомые звонки ещё могут пройти. | Все незнакомые звонки заглушаются или проходят проверку. Перед включением обязательно сохранить врача, поликлинику, доставку и другие важные номера. |

ПАМЯТКА 1

# Главная памятка владельцу телефона

Эту страницу лучше держать рядом с телефоном

**Запомните одну фразу**

«Я ничего не сообщаю по телефону. Я сейчас положу трубку и сам(а) перезвоню по сохранённому номеру».

| | |
|---|---|
| 1 | **Коды никому не называю.** Код из SMS, Telegram, WhatsApp, Viber, банка или электронной почты — это ключ к вашему аккаунту или деньгам. |
| 2 | **Данные карты не сообщаю.** Нельзя называть PIN, три цифры с обратной стороны карты, пароль, логин и полные паспортные данные. |
| 3 | **На «безопасный счёт» деньги не перевожу.** Такого способа защиты денег для клиента не существует. Не передавайте наличные курьеру и не снимайте деньги по указанию звонящего. |
| 4 | **При угрозах и спешке кладу трубку.** Фразы «прямо сейчас», «никому не говорите», «на вас оформляют кредит», «ваш родственник в беде» — повод немедленно прекратить разговор. |
| 5 | **Приложения по просьбе звонящего не устанавливаю.** Нельзя включать демонстрацию экрана, удалённый доступ, камеру у банкомата или «проверку телефона». |
| 6 | **Ссылки и QR-коды от незнакомых не открываю.** Даже если обещают выплату, подарок, возврат денег, голосование или просят подтвердить аккаунт. |
| 7 | **Знакомое имя ещё ничего не доказывает.** Аккаунт родственника могут взломать, фотографию и голос — подделать. Перезвоните родственнику по сохранённому номеру. |
| 8 | **Сомневаюсь — ничего не делаю.** Позвоните доверенному человеку. Настоящий банк, врач или сотрудник организации разрешит вам спокойно проверить информацию. |

Не перезванивайте на номер из подозрительного сообщения. Найдите официальный номер на банковской карте, договоре или ранее сохраните его в контактах.

**Если мошенничество уже произошло: немедленно звоните в милицию по номеру 102.**

ПАМЯТКА 2

# Чек-лист помощника: базовая настройка телефона

Выполняется один раз, затем проверяется каждые 6 месяцев

**Перед строгой фильтрацией звонков**
Сначала сохраните в контактах родственников, врача, поликлинику, социальную службу, банк, мобильного оператора, коммунальные службы и другие действительно важные номера.

## Защита самого телефона

☐ Установить обновления системы и всех приложений только через Google Play или App Store.

☐ Установить блокировку экрана: код не короче 6 цифр и отпечаток пальца или Face ID. Не использовать дату рождения и одинаковые цифры.

☐ Автоблокировка экрана — через 30–60 секунд.

☐ Скрыть текст уведомлений на заблокированном экране: показывать содержимое только после разблокировки.

☐ На Android запретить установку из неизвестных источников; включить проверку приложений Play Protect.

☐ Удалить ненужные приложения удалённого доступа и демонстрации экрана. Не удалять неизвестное системное приложение без проверки специалистом.

## Защита аккаунтов

☐ Включить двухэтапную проверку в Telegram, WhatsApp и Viber; добавить действующий адрес электронной почты для восстановления.

☐ Проверить разделы «Устройства», «Связанные устройства», «Компьютеры и планшеты» и отключить всё неизвестное.

☐ Пароли, PIN приложений и резервные данные не хранить в незаблокированных заметках, фотографиях или переписке. Допустим бумажный запечатанный конверт дома.

☐ Удалить публичное имя пользователя Telegram, если оно не нужно, и не публиковать номер телефона, адрес, документы и банковские реквизиты в профиле.

## Проверка после настройки

☐ Позвонить с сохранённого номера: телефон и нужные мессенджеры должны звонить.

☐ Позвонить с несохранённого номера: результат должен соответствовать выбранному режиму.

☐ Показать владельцу, где находятся пропущенные неизвестные звонки и папки «Запросы»/«Спам». Объяснить: самостоятельно не перезванивать.

☐ Договориться о семейном кодовом слове для экстренных просьб. Не записывать его в телефон, эту методичку или рядом с банковскими данными.

ПАМЯТКА 3

# Обычные телефонные звонки: Android и iPhone

Сначала включаем штатную защиту, без сомнительных «антиспам»-приложений

## Android: приложение «Телефон» от Google

| Где открыть | Что установить и зачем |
|---|---|
| **Телефон → ⋮ → Настройки → АОН и спам** | **Показывать данные абонента и спам — ВКЛ.**<br>Телефон будет помечать известные подозрительные номера. |
| **Там же** | **Фильтровать спам-звонки — ВКЛ., если пункт доступен.**<br>Подозрительные звонки могут не подавать сигнал, но останутся в журнале. |
| **Журнал звонков → подозрительный номер** | **Заблокировать / сообщить о спаме.**<br>Блокируйте каждый повторяющийся подозрительный номер. |
| **Телефон → Настройки → Заблокированные номера** | **Не полагаться только на переключатель «Неизвестные».**<br>В приложении Google он блокирует скрытые/неопределённые номера, но не все номера, которых нет в контактах. |

На Samsung, Xiaomi, Honor и других марках названия отличаются. Ищите «АОН и защита от спама», «Антиспам», «Блокировка мошеннических звонков». Не устанавливайте случайное приложение по рекламе или совету звонящего.

## iPhone

| Где открыть | Что установить и зачем |
|---|---|
| **Настройки → Приложения → Телефон → Проверка неизвестных абонентов** | **«Спросить причину звонка» — предпочтительный компромисс.**<br>Незнакомого абонента сначала попросят назвать причину звонка; функция зависит от версии системы и региона. |
| **Там же** | **«Заглушать» — максимальный режим.**<br>Незнакомые номера не звонят и направляются на голосовую почту. Можно пропустить врача, доставку или организацию. |
| **Телефон → Фильтрация вызовов** | **«Неизвестные абоненты» и «Спам» — ВКЛ., если доступны.**<br>Спам-фильтр оператора может зависеть от страны и тарифа. |
| **Настройки → Уведомления → Показ миниатюр** | **«Если разблокировано».**<br>Текст SMS и кодов не будет виден постороннему на заблокированном экране. |

**После включения максимального режима**

Научите владельца не перезванивать по неизвестным пропущенным номерам. Настоящая организация обычно оставит понятное сообщение; проверять её нужно через официальный сохранённый номер.

ПАМЯТКА 4

# Telegram: рекомендуемые настройки

Цель: скрыть номер, ограничить звонки и защитить вход

Основной путь: Telegram → Настройки → Конфиденциальность (или «Конфиденциальность и безопасность»).

| Где открыть | Что установить и зачем |
|---|---|
| **Номер телефона** | **Кто видит мой номер — Никто.**<br>Люди, которые уже знали номер и сохранили его, всё равно могут его видеть. |
| **Номер телефона** | **Кто может найти меня по номеру — Мои контакты.**<br>Случайному человеку будет сложнее связать введённый номер с вашим профилем. |
| **Последняя активность и статус «В сети»** | **Мои контакты.**<br>Незнакомые не увидят привычный режим активности. |
| **Фотографии профиля** | **Мои контакты.**<br>Лучше не ставить фото документов, дома, билетов или банковских карт. |
| **Звонки** | **Мои контакты; в максимальном режиме — Никто.**<br>Перед строгим режимом сохраните всех близких. |
| **Группы и каналы / Приглашения** | **Мои контакты.**<br>Снижает риск добавления в мошеннические группы. |
| **Двухэтапная аутентификация** | **Включить отдельный пароль и почту восстановления.**<br>Код из SMS или Telegram сам по себе не позволит войти в аккаунт. |
| **Устройства / Активные сеансы** | **Оставить только знакомые устройства.**<br>Незнакомый сеанс немедленно завершить. |
| **Код-пароль / Блокировка приложения** | **Включить код и биометрию.**<br>Защищает переписку, если разблокированный телефон оказался у другого человека. |
| **Профиль → Изменить → Имя пользователя** | **Удалить публичное @имя, если оно не нужно.**<br>По публичному имени и общей группе незнакомые могут найти профиль без номера телефона. |

### Никогда не сообщайте код Telegram

Коды входа в Telegram приходят в служебный чат Telegram или по SMS. Их нельзя диктовать «службе поддержки», родственнику, банку или вводить на чужом сайте.

- Незнакомый чат: не отвечать, не нажимать «Start» у подозрительного бота, не открывать файл или ссылку.
- Открыть профиль отправителя → Заблокировать; для мошеннического сообщения также выбрать «Пожаловаться».

ПАМЯТКА 5

# WhatsApp: рекомендуемые настройки

Цель: заглушить незнакомые звонки, скрыть данные и защитить вход

Основной путь: WhatsApp → Настройки → Конфиденциальность. Сначала откройте «Проверка конфиденциальности» и пройдите все разделы.

| Где открыть | Что установить и зачем |
|---|---|
| **Конфиденциальность → Звонки** | **Заглушать неизвестных абонентов — ВКЛ.**<br>Такие звонки не подают сигнал, но остаются в списке звонков. |
| **Конфиденциальность → Группы** | **Мои контакты.**<br>Незнакомые не смогут напрямую добавлять владельца в большинство групп. |
| **Время последнего посещения и «В сети»** | **Мои контакты; статус «В сети» — как время посещения.**<br>Снижает объём видимой незнакомым информации. |
| **Фото профиля** | **Мои контакты.**<br>Не использовать фото документов, билетов и банковских карт. |
| **Сведения** | **Мои контакты или Никто.**<br>Не указывать адрес, место работы, дату рождения и другую лишнюю информацию. |
| **Статус** | **Мои контакты.**<br>Проверить исключения и удалить незнакомых. |
| **Конфиденциальность → Расширенные** | **Защищать IP-адрес во время звонков — ВКЛ.**<br>Звонки будут проходить через серверы WhatsApp; качество иногда может немного снизиться. |
| **Там же, если доступно** | **Отключить предпросмотр ссылок — ВКЛ.; блокировать большой объём сообщений от неизвестных аккаунтов — ВКЛ.**<br>Названия новых пунктов зависят от версии приложения. |
| **Настройки → Аккаунт → Двухшаговая проверка** | **Включить PIN/пароль и добавить почту восстановления.**<br>Никому не сообщать этот PIN, даже если человек знает имя владельца. |
| **Настройки → Связанные устройства** | **Отключить все неизвестные компьютеры и телефоны.**<br>Проверять после любого подозрительного QR-кода или просьбы «подтвердить устройство». |

### Не сканируйте QR-код по просьбе незнакомца

QR-код может подключить чужой компьютер к вашему WhatsApp. Подключение допустимо только на своём компьютере и при осознанном открытии функции «Связанные устройства».

- Неизвестный отправитель: не продолжать разговор → «Заблокировать» и «Пожаловаться».
- Просьбу знакомого перевести деньги всегда проверять обычным звонком на ранее сохранённый номер.

ПАМЯТКА 6

# Viber: рекомендуемые настройки

Цель: отделить неизвестные сообщения, ограничить группы и защитить вход

Основной путь: Viber → Ещё → Настройки → Конфиденциальность.

| Где открыть | Что установить и зачем |
|---|---|
| **Двухэтапная проверка** | **Включить PIN и добавить почту восстановления.** PIN потребуется при активации Viber на другом телефоне. |
| **Кто может добавлять в группы** | **Мои контакты.** Настройка относится к обычным группам; сообщества могут работать иначе. |
| **Запросы на переписку** | **ВКЛ.** Неизвестные сообщения попадут в отдельный раздел, где доступны «Удалить» или «Заблокировать и пожаловаться». Функция может быть недоступна в отдельной стране. |
| **Заглушать звонки от несохранённых номеров** | **ВКЛ. на Android.** По официальной справке Viber эта автоматическая функция доступна только на Android. |
| **Автоматическая проверка спама** | **ВКЛ., если пункт доступен.** Viber проверяет сообщения от людей не из контактов на вредоносное содержимое. |
| **Статус «В сети», просмотр сообщений, фото, день рождения** | **Максимально ограничить; фото и дату рождения скрыть от незнакомых.** Некоторые переключатели взаимны: скрыв свой статус, владелец может перестать видеть чужой. |
| **Ещё → Настройки → Аккаунт → Компьютеры и планшеты** | **Отключить все неизвестные устройства.** Особенно после сканирования QR-кода или использования чужого компьютера. |
| **Подозрительный чат/звонок** | **Заблокировать и пожаловаться.** После блокировки пользователь не сможет писать и звонить. |

### Не нажимайте «Принять» в запросе незнакомца

Пока запрос не принят, отправитель не видит ваш статус «В сети» и отметку о прочтении. Для подозрительного запроса выбирайте «Заблокировать и пожаловаться», а не просто «Удалить».

На iPhone Viber не предоставляет общего автоматического заглушения всех звонков от несохранённых номеров. Используйте системную проверку неизвестных звонков iPhone и блокировку внутри Viber.

ПАМЯТКА 7

# Что делать при подозрительном звонке или сообщении

Простой порядок действий без споров и проверки личности в разговоре

| | |
|---|---|
| 1 | **Остановитесь.** Не нажимайте кнопки, не открывайте ссылку, не диктуйте сведения и не выполняйте указания. |
| 2 | **Положите трубку.** Не нужно убеждать мошенника, спорить с ним или ждать «переключения на сотрудника». |
| 3 | **Проверьте другим способом.** Позвоните родственнику, банку или организации самостоятельно — только по сохранённому официальному номеру. |
| 4 | **Посоветуйтесь.** При малейшем сомнении позвоните доверенному человеку до совершения любого действия с деньгами или аккаунтом. |
| 5 | **Заблокируйте и пожалуйтесь.** Сделайте это в приложении; подозрительный номер обычного телефона отметьте как спам. |
| 6 | **Сохраните доказательства.** Не удаляйте сообщение до проверки: сделайте скриншот, сохраните номер, ссылку, время звонка и реквизиты перевода. |

## Признаки мошенничества

- Просят код, пароль, PIN, данные карты, фото документа или доступ к экрану.
- Запрещают советоваться с родственниками, банком или милицией.
- Торопят, пугают уголовным делом, потерей денег, блокировкой телефона или аккаунта.
- Просят перевести деньги, купить криптовалюту, подарочные сертификаты, передать наличные курьеру.
- Просят установить приложение, включить демонстрацию экрана, поднести карту к телефону или подойти к банкомату.
- Сообщают о «выигрыше», «компенсации», «перерасчёте», «доставке» или «голосовании» и присылают ссылку.

**Даже номер банка или знакомого может быть подменён**

Не доверяйте только имени на экране, фотографии или голосу. Надёжная проверка — завершить контакт и самостоятельно набрать сохранённый номер.

ПАМЯТКА 8

# Если уже сообщили код, перевели деньги или дали доступ

Действуйте сразу, но с другого безопасного устройства

**Если на телефоне включён удалённый доступ или демонстрация экрана**
Не вводите на нём новые пароли и банковские данные. Включите авиарежим, выключите Wi-Fi и используйте другой доверенный телефон или компьютер для связи с банком и смены паролей.

**ПЕРВЫЙ ШАГ: НЕМЕДЛЕННО ПОЗВОНИТЕ В МИЛИЦИЮ ПО НОМЕРУ 102.**

☐ **Немедленно позвонить в милицию по номеру 102 и сообщить, что произошло.**

☐ Немедленно позвонить в банк по номеру с карты или официального сайта: сообщить о мошенничестве, заблокировать карты/счета и оспорить операции, если это возможно.

☐ С безопасного устройства сменить пароль электронной почты, затем банков, Telegram, WhatsApp и других важных сервисов. Везде завершить неизвестные сеансы.

☐ Telegram: Настройки → Устройства / Активные сеансы → завершить чужие сеансы; включить двухэтапную аутентификацию.

☐ WhatsApp: Настройки → Связанные устройства → выйти на неизвестных устройствах; проверить двухшаговую проверку.

☐ Viber: Ещё → Настройки → Аккаунт → Компьютеры и планшеты → деактивировать неизвестные устройства; проверить PIN.

☐ Если SIM-карта внезапно перестала работать или приходят сообщения о её замене — срочно связаться с мобильным оператором с другого телефона.

☐ С помощью специалиста удалить приложение удалённого доступа и проверить специальные возможности, администратора устройства, профили управления и разрешение «поверх других окон».

☐ Сохранить скриншоты, номера, ссылки, чеки и время событий; обратиться в банк и позвонить в милицию по номеру 102. Не платить «помощникам по возврату денег».

Не стыдитесь и не скрывайте случившееся. Чем раньше банк, оператор и близкие узнают о происшествии, тем больше возможностей ограничить ущерб.