

ПАМЯТКА ПО ОСНОВНЫМ ПРАВИЛАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБЩИЕ СОВЕТЫ

Не переходите по ссылкам, особенно про различные голосования и помощь детям. Если вам пришла такая ссылка от знакомого, позвоните ему.

Не сообщайте никому коды подтверждения, не отправляйте свои пароли.

Не переводите деньги по просьбе знакомых без предварительного разговора. Имейте в виду, что современные технологии могут подменять голос и видео. Крупные суммы передавайте лично в руки, с оформлением договора и под расписку.

Не сообщайте никому данные карт, не храните рядом с картами их ПИН-коды. Не вводите данные от личного кабинета, мобильного приложения или ПИН-код на клавиатуре банкомата в присутствии постороннего. При вводе прикрывайте клавиатуру рукой. Не совершайте платежи на подозрительных сайтах и незнакомых платежных платформах.

При утере или краже банковской карты, а также при обнаружении операции, которую не совершали, следует незамедлительно связаться с банком и заблокировать карту (через мобильное приложение, интернет-банк или позвонив на горячую линию). При подозрительном списании нужно подать заявление не только о блокировке, но и об отзыве перевода. Нелишним будет и обращение в полицию с заявлением о мошеннических действиях.

Если вы потеряли карту и вам её вернули, или вы оставили её на прилавке магазина, а потом забрали, то не продолжайте пользоваться этой картой – она уже скомпрометирована. Лучше заблокируйте её и выпустите новую.

Официальные представители Центробанка, ФСБ, МВД, прокуратуры и других госорганов НИКОГДА НЕ БУДУТ ЗВОНИТЬ по официальным служебным вопросам на личные сотовые телефоны граждан, не будут ничего присылать вам или запрашивать от вас какую-либо официальную информацию через любые ИНОСТРАННЫЕ сервисы или мессенджеры.

Любые странные сообщения и СМС с неизвестных номеров, особенно с вложенными файлами или ссылками – игнорируйте, не открывайте вложения и лучше сразу удаляйте.

Используйте только СЛОЖНЫЕ пароли, РАЗНЫЕ ДЛЯ РАЗНЫХ учетных записей и сервисов. Пользователи, которые используют один и тот же пароль для всех сервисов, при компрометации хотя бы одного из сервисов могут потерять доступ ко всем своим учетным записям. По возможности, во всех доступных сервисах используйте двухфакторную аутентификацию («логин и пароль» + «код из СМС или электронной почты»).

Внимательно читайте предупреждения на компьютере и телефоне, не подтверждайте и не нажимайте на «ОК» без понимания сути сообщения.

Обязательно поставьте ПИН-код на SIM-карту, чтобы обезопасить свой номер и всё, что к нему привязано, при утере телефона.

Whatsapp

Двухшаговая проверка

Двухшаговая проверка — это дополнительная функция, которая усиливает защиту вашего аккаунта WhatsApp. После успешной регистрации номера телефона в WhatsApp откроется экран двухшаговой проверки. При включении двухшаговой проверки вы можете указать свой адрес электронной почты. Это поможет защитить ваш аккаунт и позволит вам получить ссылку для сброса PIN-кода WhatsApp по электронной почте, если вы его забудете.

После подключения двухшаговой проверки WhatsApp будет регулярно просить вас ввести PIN-код в качестве напоминания. Вы будете получать напоминание раз в неделю, пока не решите сбросить PIN-код.

Ни с кем не делитесь своим шестизначным кодом, полученным при регистрации номера, или PIN-кодом для двухшаговой проверки.

ПАМЯТКА ПО ОСНОВНЫМ ПРАВИЛАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Если вы не включали двухшаговую проверку, но получили запрос на ввод PIN-кода, вероятно, эту функцию включил предыдущий владелец вашего телефонного номера. В этом случае вы сможете сбросить PIN-код и получить доступ к своему аккаунту через 7 дней.

Если вы забыли свой PIN-код и успешно зарегистрировали свой номер телефона в WhatsApp, нажмите **Забыли PIN-код?**, чтобы создать новый. Вы можете в любое время изменить параметры двухшаговой проверки с помощью PIN-кода в настройки WhatsApp > **Аккаунт** > **Двухшаговая проверка**.

Как обезопасить свой аккаунт

Чтобы обеспечить безопасность своего аккаунта WhatsApp, воспользуйтесь приведёнными ниже рекомендациями.

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.

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.

Если вы получите электронное письмо для сброса PIN-кода двухшаговой проверки или кода регистрации, которое не запрашивали, не нажимайте ни на какие ссылки. Возможно, кто-то пытается получить доступ к вашему номеру телефона в WhatsApp.

Вы получили код подтверждения, хотя не запрашивали его

Для защиты вашего аккаунта WhatsApp отправит вам уведомление, если кто-либо попытается зарегистрировать аккаунт WhatsApp с вашим номером телефона. Чтобы ваш аккаунт оставался в безопасности, не делитесь своим кодом подтверждения ни с кем.

Если вы получили такое уведомление, это означает, что кто-то ввёл ваш номер телефона и запросил код подтверждения. Это нередко происходит, когда другой пользователь ошибается при вводе своего номера, но это также может произойти и в том случае, если кто-то пытается завладеть вашим аккаунтом.

Ни в коем случае не делитесь своим кодом подтверждения WhatsApp с другими. Если кто-либо пытается украсть ваш аккаунт, ему понадобится код подтверждения из SMS, отправленного на ваш номер. Пользователь, пытающийся подтвердить ваш номер телефона, не сможет пройти процесс подтверждения без этого кода и воспользоваться вашим номером в WhatsApp. Это значит, что вы по-прежнему будете контролировать свой аккаунт WhatsApp.

Telegram

Настройте двухфакторную авторизацию

Двухфакторная авторизация в Telegram позволяет значительно повысить уровень безопасности. При подключении к вашей учетной записи нового устройства — смартфона, ноутбука или планшета — нужно подтверждать авторизацию двумя разными способами.

Включение облачного пароля — отличное решение для этого. Даже если злоумышленник сможет войти по коду из смс, ему потребуется ввести еще уникальный пароль, известный только владельцу.

Настроить эту функцию несложно. Откройте на своем смартфоне или ноутбуке Telegram, перейдите в «Настройки — Конфиденциальность — Облачный пароль». Задайте удобный запоминающийся пароль, подсказку к нему (на всякий случай), а потом укажите адрес электронной почты. Теперь ваша учетная запись защищена гораздо лучше.

Скройте номер телефона от посторонних

Не стоит показывать всем номер телефона, привязанный к учетной записи Telegram. Злоумышленники могут использовать его для спама или попыток взлома.

Чтобы скрыть номер, необходимо снова перейти в «Настройки», выбрать «Конфиденциальность», а затем открыть пункт «Номер телефона». Там можно либо полностью скрыть номер от посторонних глаз, либо настроить списки доступа.

ПАМЯТКА ПО ОСНОВНЫМ ПРАВИЛАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проверяйте привязанные устройства

В настройках мессенджера можно увидеть, какие устройства имеют доступ к вашей учетной записи. Если вы заходите в Telegram со смартфона, рабочего ноутбука и домашнего ПК, все эти сеансы будут там видны. Telegram покажет даже город, в котором было подключение, и примерное время.

Не удалось распознать подозрительное устройство? Лучше сразу его удалить. Не обязательно это злоумышленник — возможно, вы просто однажды зашли в свою учетную запись с рабочего телефона, а потом забыли об этом. Но осторожность не помешает.

Чтобы проверить список сеансов, перейдите в «Настройки — Конфиденциальность — Устройства». А еще здесь можно подключить новое устройство через QR-код или настроить завершение сеансов, если они слишком долго не были активными.

Будьте внимательны

Никакая двухфакторная защита не спасет, если владелец учетной записи Telegram сам передаст злоумышленнику необходимые данные для взлома. Не стоит пользоваться подозрительными чат-ботами, если не уверены в их надежности. Также не желательно принимать участие в различных онлайн-голосованиях, которые присылают в личные сообщения. Иногда приславший даже не подозревает, что его ссылка небезопасна, и тоже становится жертвой «угона». Наконец, не следует авторизоваться на неизвестных сайтах через телеграм-аккаунт.