Дорогой друг!

🔐 **Мир цифровой, но ловушки в нём реальны. Защищай свои данные и делись знаниями с близкими.**

- ☐ Сделай свой профиль приватным — ограничь доступ к постам и данным только для друзей.
- ☐ Удали из профиля и постов личные данные: телефон, адрес, дату рождения, электронную почту.
- ☐ Включи двухфакторную аутентификацию (2FA) — дополнительную защиту аккаунтов с помощью кода из SMS или приложения.
- ☐ Отключи геолокацию в социальных сетях и приложениях, чтобы не раскрывать своё местоположение.
- ☐ Публикуй только безопасные фотографии — без билетов, документов, карт и табличек с адресом.
- ☐ Используй разные сложные пароли для каждого сайта и приложения.
- ☐ Храни пароли вне браузера — используй менеджеры паролей для безопасности.
- ☐ Переходи по проверенным и надёжным ссылкам, избегай сомнительных источников.
- ☐ Будь внимателен к запросам и предложениям в интернете — не доверяй подозрительным сообщениям.
- ☐ Регулярно обновляй программное обеспечение и антивирусные программы.
- ☐ Обучай друзей и близких основам цифровой безопасности.
- ☐ При подозрении на мошенничество — сообщи в соответствующие службы
- ☐ Регулярно проверяй активные сеансы и устройства — следи за тем, с каких устройств и где был выполнен вход в аккаунт, и выходи из подозрительных сеансов.
- ☐ Используй надёжные антивирусы и VPN — дополнительная защита при работе в интернете, особенно в общедоступных сетях.
- ☐ Создай резервные копии важных данных, чтобы восстановить информацию в случае потери доступа или атаки.
- ☐ Проверь настройки конфиденциальности приложений — не только социальных сетей, но и мессенджеров, почты, облачных сервисов.

🛡️ **Защити себя сегодня — начни с простых шагов! Поделись этим чек-листом с друзьями и семьёй, чтобы они тоже были в безопасности.**

- Двухфакторная аутентификация (2FA) — дополнительный уровень защиты: помимо пароля, для входа требуется код из SMS или приложения-аутентификатора.
- Геолокация — отключай в приложениях и социальных сетях, если она не нужна. Фото с геотегами могут раскрыть местоположение и распорядок дня.
- Пароли — используй уникальные и сложные пароли для каждого сайта. Менеджеры паролей помогут их генерировать.
- Безопасность паролей — избегай хранения паролей в браузере, особенно на общих или незащищённых устройствах.
- Подозрительные ссылки — избегай ссылок из неизвестных источников и сомнительных сообщений.
- Обновления ПО — своевременное обновление операционной системы, браузера и антивируса защищает от новых угроз.
- Сообщение о мошенничестве — при подозрительной активности обращайся в службу поддержки социальных сетей, банков или правоохранительных органов.

contact.oversilence@yandex.ru