

Чек лист: проверь уровень цифровой гигиены для себя и команды

1. Аккаунты и доступы

- Для разных сервисов используются разные пароли
- Пароли хранятся в менеджере паролей, а не в записках
- Двухфакторная аутентификация включена для почты, банковских сервисов и соцсетей

2. Устройства

- Автоматические обновления системы и приложений включены
- Экран устройств блокируется паролем, PIN-кодом или биометрией
- Настроено резервное копирование важных данных

3. Почта и ссылки

- Отправитель и домен письма проверяются перед открытием вложений
- Подозрительные файлы и ссылки не открываются
- Срочные запросы перепроверяются, а не выполняются автоматически

4. Социальные сети и мессенджеры

- Настройки приватности ограничивают доступ к личным данным
- Коды подтверждения никому не передаются
- Осознанно публикуется только та информация, которая допустима публично

5. Сети и Wi-Fi

- Финансовые операции и входы в сервисы не выполняются через открытые сети
- Стандартный пароль роутера дома / в офисе изменен и сохранен в надежном месте

6. Команда и коммуникации

- Доступы выданы по ролям и пересматриваются при изменении задач
- Зафиксированы правила работы в сети и передачи данных
- Сотрудники знают, куда обращаться при подозрении на инцидент