Памятка: безопасные пароли и двухфакторная аутентификация (2FA)

Рекомендуется для всех классов (6–11).

Какой пароль считается надёжным

- Длина 12–16 символов и больше.
- Уникальный для каждого сервиса.
- Используй фразу-пароль (несколько слов) — так проще запомнить.
- Не используй дату рождения, имя, номер телефона.

2FA — зачем и как

2FA добавляет второй шаг входа (код из приложения/смс/ключ безопасности). Даже если пароль украдут, без второго фактора войти сложнее.

- Предпочтительно: приложение-аутентификатор (TOTP).
- Храни резервные коды отдельно (в бумажном виде или менеджере).
- Никому не сообщай коды подтверждения.

Чек-лист

Действие	Сделано
Сменил(а) пароль в основном аккаунте	☐
Включил(а) 2FA в соцсети	☐
Включил(а) 2FA в почте	☐
Проверил(а) активные сессии и вышел(ла) из лишних	☐

PDF можно распечатать и выдать как памятку. Рекомендуется обновлять раз в полугодие.