Чек-лист: как защитить пароли и аккаунты

Из курса Учебника Т—Ж
«Как защититься от мошенников»

- [ ] **Относиться к паролям как к ключам от квартиры.** Никому не сообщать пароли, пин-коды и коды из смс
- [ ] **Придумывать длинные и сложные пароли, в первую очередь — для почты.** Использовать не менее 14 символов, добавлять слова, образы и ассоциации вместо простых комбинаций
- [ ] **Использовать разные пароли для разных сервисов.** Не повторять их, чтобы утечка одного не дала доступ ко всем аккаунтам
- [ ] **Применять простой алгоритм для запоминания паролей.** Брать базовую фразу и модифицировать ее под каждый сайт, чтобы не запоминать все с нуля
- [ ] **Проверять сайт перед вводом пароля.** Внимательно читать адрес, обращать внимание на домен, странные символы и наличие HTTPS
- [ ] **Использовать менеджер паролей.** Хранить пароли в зашифрованном виде и полагаться на автоподстановку как индикатор подлинности сайта
- [ ] **Не хранить пароли в небезопасных местах:** не записывать их в заметках, на стикерах, не класть в бумажник
- [ ] **Включить двухфакторную аутентификацию,** чтобы одного пароля было недостаточно для входа
- [ ] **Не сообщать коды из смс и писем,** даже если их просят под предлогом безопасности или восстановления доступа
- [ ] **Установить пин-код на сим-карту,** чтобы злоумышленник не смог получить доступ к смс при краже телефона
- [ ] **Сохранять критичность и брать паузу.** Не действовать под давлением, проверять любые подозрительные запросы и не спешить передавать данные

Читайте курсы Учебника Т—Ж и делитесь нашими материалами.
Подробнее о том, как защититься от мошенников: **https://t-j.ru/pro/bezopasnost/**