ФГАОУ ВО «КФУ им. В.И. Вернадского»

Физико-технический институт (структурное подразделение)

Кафедра компьютерной инженерии и моделирования

Отчет на тему

# «Цифровая гигиена и личная безопасность в интернете»

|  |
| --- |
| Выполнил: студент 1 курса группы ПИ-б-о-241(2)  Османов Асан Фаррухович |
| Проверил:  Заведующий  кафедрой компьютерной инженерии и моделирования Милюков В. В. |

Симферополь, 2025

**Цель:**

Основной задачей стало донести до членов моей семьи и друзей важность осознанного поведения в цифровом пространстве. Мы обсудили основные виды мошенничества, наиболее распространённые сценарии атак и способы их предотвращения.

**Темы, поднятые в беседе:**  
В ходе встречи я представил доступные материалы и слайды, на которых были наглядно показаны различные схемы киберпреступников. Мы рассмотрели такие угрозы, как:

* Инсценировки аварий с участием родственников
* Мошеннические звонки от имени руководства
* Ложные обращения от банковских сотрудников
* Перехват и использование аккаунтов в соцсетях
* Поддельные сайты и вредоносные программы
* Опасности при использовании смартфонов
* Фишинговые письма
* Ложные предложения о работе
* Фальсифицированные звонки от операторов связи
* Иные распространённые уловки мошенников

**Практические советы для родных**  
После обсуждения примеров каждый участник получил пошаговые инструкции по противодействию угрозам. Важно:

* Перепроверять достоверность сообщений и звонков, особенно если просят действовать срочно.
* Всегда использовать двухфакторную аутентификацию там, где это возможно.
* Не вводить личные данные на незнакомых сайтах.
* Следить за обновлениями ПО и антивирусных решений.
* Осторожно относиться к письмам и ссылкам от неизвестных отправителей.
* Игнорировать просьбы сообщить личную информацию, даже если просят от имени государственных структур.

**Основные выводы**  
В процессе подготовки и общения я пришел к следующим ключевым урокам:

1. **Бдительность** — всегда сомневаться в запросах на конфиденциальную информацию.
2. **Сдержанность** — не принимать поспешных решений под давлением.
3. **Дополнительная защита** — 2FA как стандарт безопасности.
4. **Осторожность в интернете** — ограниченное использование банковских карт для покупок.
5. **Техническая дисциплина** — обновления и антивирус — обязательны.
6. **Анализ источников** — внимательное отношение к ссылкам и письмам.
7. **Обучение других** — делиться знаниями, особенно с пожилыми людьми.

**Рекомендации по предотвращению обмана**  
Чтобы обезопасить себя от обмана, важно:

* Быть внимательным к неожиданным контактам.
* Всегда уточнять, кто именно запрашивает информацию.
* Использовать виртуальные карты и одноразовые коды.
* Держать под рукой официальные контакты служб.
* Постоянно повышать уровень цифровой грамотности.
* Пользоваться проверенным антивирусным ПО.

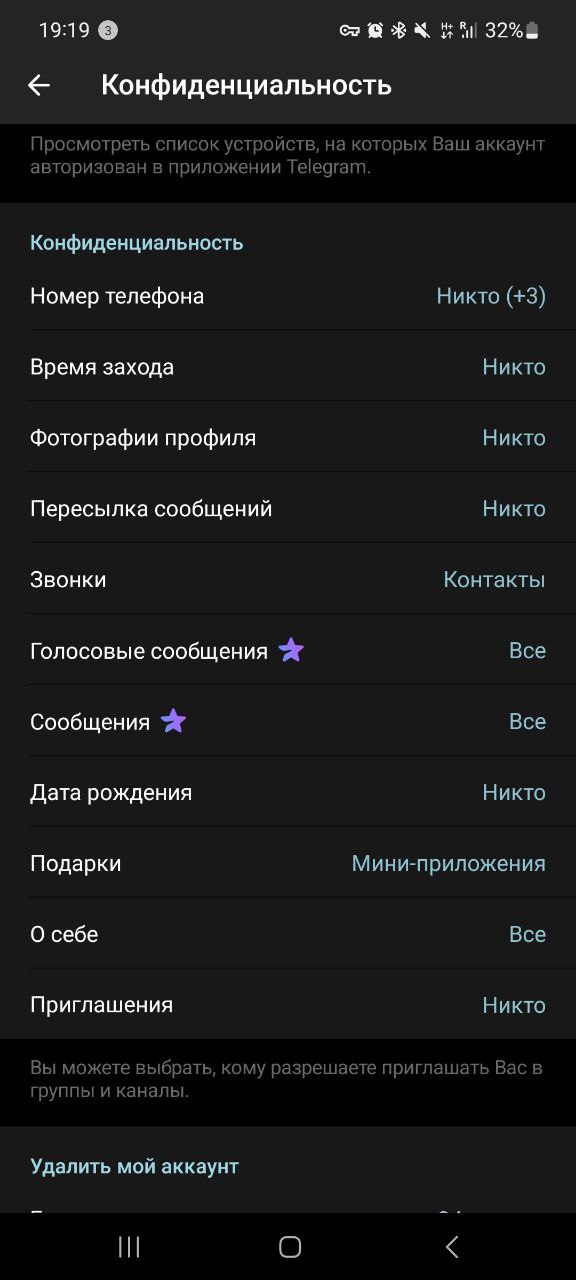
**Современные угрозы и способы их распознавания**  
Кибермошенники используют не только технику, но и психологию:

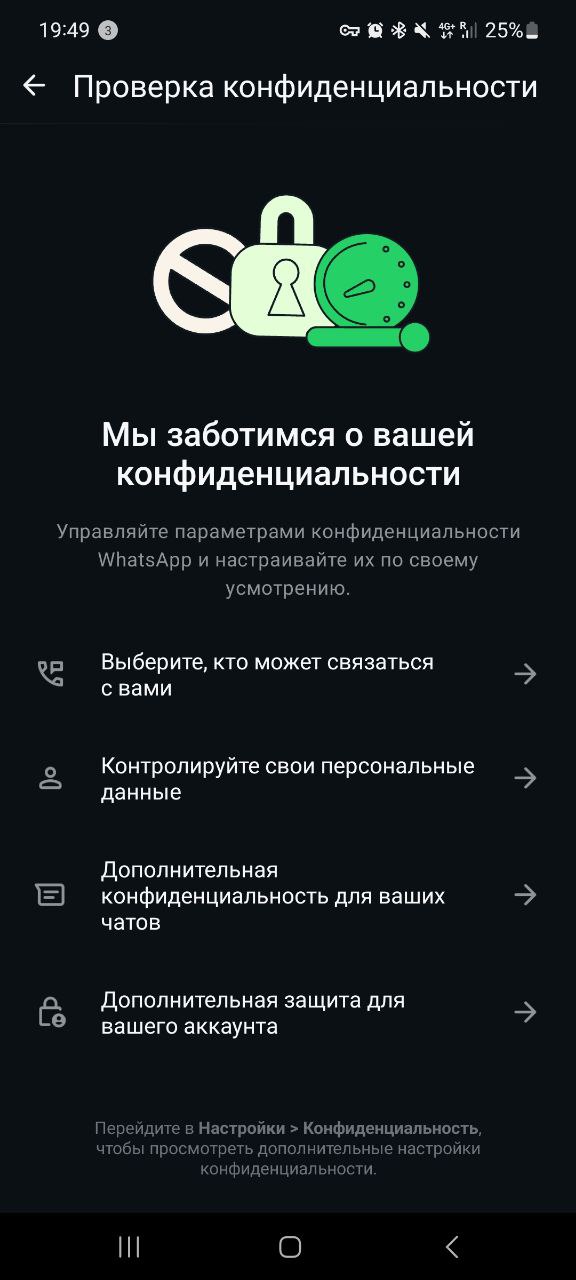
* **Дипфейки** могут подделывать голос родных.
* **Вредоносные приложения** — под маской полезных программ.
* **Фальшивые уведомления** — пытаются ввести в заблуждение через страх или срочность.

**Как себя обезопасить:**

* Не открывайте файлы от неизвестных.
* Очищайте кэш браузера.
* Проверяйте, совпадает ли адрес сайта с официальным.

**Реальные случаи и решения:**

* **С родственником:** после серии мошеннических звонков мы настроили звонки в телеграм только контактам.  
  Telegram:  
  

Whatsapp:  
Помимо настройки звонков, также принял дополнительные меры безопасности.  


* **С другом:** ложное сообщение о том, что близкий родственник в опасности. Решение: Позвонил родственнику и спросил все ли в порядке.

**Заключение**  
Интернет — мощный инструмент, но только при ответственном использовании. Регулярная профилактика, знания и внимательность — основа кибербезопасности. Защищая себя, мы автоматически защищаем и своих близких.