

ОТДЕЛЬНЫЙ УРОК · ЦИФРОВАЯ ШКОЛА

Сообщения, звонки и вложения

Проверяем знакомых, неожиданные файлы и просьбы показать экран.



Учебная иллюстрация

- Проверить необычную просьбу и не выдать доступ через вложение, голос или трансляцию экрана.

Иван Юрьевич

learn.ivan-it.net

Версия 1.0 · Редакционная проверка: 2026-10-26

Можно читать без интернета, отмечать на бумаге и возвращаться к нужной ситуации.
Кликабельные ссылки и адреса ведут к материалам и официальным источникам.

Название проекта рабочее. Материал авторский, не государственная программа. Не вводите настоящие пароли и коды в учебные задания.

УРОК 1

Сообщения, звонки и вложения

Проверяем знакомых, неожиданные файлы и просьбы показать экран.

Версия 1.0 · Редакционная проверка: 2026-10-26



Учебная иллюстрация

Если сообщение торопит

1

Сделайте паузу

2

Свяжитесь знакомым
способом

3

Решайте после проверки

Смысловая схема по материалу. Действия и ограничения подробно описаны ниже.

Что вы сможете сделать

Проверить необычную просьбу и не выдать доступ через вложение, голос или трансляцию экрана.

Учебный пример

Учебный пример. Из привычного аккаунта знакомого приходит «Твои фото» и файл, который телефон предлагает установить как приложение. Получатель не устанавливает его и связывается со знакомым по прежнему номеру. История показывает несоответствие обещанного материала и фактического действия.

Знакомый аккаунт и новая просьба

Имя и фотография профиля помогают узнать человека, но не подтверждают, кто сейчас управляет перепиской. Аккаунт могли скопировать, получить к нему доступ или использовать пересланное сообщение без понимания содержания. Особенно внимательно проверяйте внезапные просьбы о деньгах, кодах, установке программы и сохранении тайны. Проверять полезно и знакомого, и само необычное действие.

Остановите переписку и используйте ранее известный другой контакт: сохранённый номер, личную встречу, привычного общего знакомого. Вопрос «это точно ты?» в том же чате не создаёт новой проверки. Если сообщение оказалось чужим, предупредите настоящего владельца и близких спокойным фактом: от аккаунта идут необычные просьбы. Не публикуйте без необходимости личную переписку и предположения о виновнике.

Голос и видео тоже требуют проверки

Узнаваемый голос и лицо усиливают доверие. Однако запись можно вырвать из контекста, а технологии позволяют создавать убедительные подделки. Это не значит, что каждое видео ненастоящее. Для важного решения достаточно сохранить прежнее правило: необычную просьбу подтверждают независимым способом, особенно когда собеседник торопит, запрещает перезвонить или требует совершить финансовое действие.

Не превращайте семейное кодовое слово в единственную защиту. Его могут услышать или узнать из переписки. Лучше договориться, что любое срочное поручение разрешено перепроверять и никто не обидится на обратный звонок. Если родственник действительно в беде, отдельная проверка помогает понять место, нужную помощь и законный способ связи, а не выполнять неизвестные указания по переводу.

Файл может делать другое, чем обещает

Вложение - переданный файл: изображение, документ, архив или программа. Значок и название выбирает отправитель. Установка приложения вместо просмотра фотографии - явное несоответствие. На Android установочный файл может иметь окончание .apk; на Windows программу запускают, например, файлы .exe. Не нужно запоминать все расширения: насторожьтесь, если система предлагает установку, выполнение или дополнительные права вместо ожидаемого чтения.

Не включайте исполняемые возможности документа, не распаковывайте неизвестный архив ради любопытства и не отключайте предупреждения защиты по просьбе отправителя. Нужный материал запросите в обычном формате или найдите у известного издателя. Скачивание ещё не тождественно запуску, а запуск - не доказательство конкретного результата. После подозрительного события важно точно вспомнить, какое действие действительно произошло.

Показывать экран - тоже передавать сведения

При демонстрации экрана собеседник видит меняющееся содержимое дисплея. Поверх обычного окна могут появиться сообщения, одноразовый код, документ или остаток на счёте. Передача видимости отличается от удалённого управления, но обе возможности требуют отдельного согласия и понятной цели. Не открывайте финансовые приложения и хранилище секретов во время неожиданной «проверки».

Если помощь нужна, заранее определите, что помощник должен увидеть, и закройте лишнее. Для простого объяснения часто достаточно описать название ошибки без снимка личных данных. Завершайте трансляцию перед вводом секретов. Не сообщайте коды подключения к удалённому управлению неизвестному мастеру и не принимайте новое разрешение автоматически: оно может дать больше возможностей, чем просмотр одного окна.

Угрозы, шантаж и нежелательное общение

Угроза опубликовать личные материалы, обвинить близкого или разрушить репутацию создаёт сильное давление. Не выполняйте требования ради обещания «тогда всё удалим»: такое обещание нельзя проверить оплатой или новой фотографией. Остановите взаимодействие и обратитесь к доверенному человеку. При непосредственной опасности сначала нужна помощь для физической безопасности, а уже затем настройки аккаунта.

Сохраните доступные сведения о контакте и времени угроз без дальнейшего распространения чувствительных материалов. Жалоба и блокировка выбираются после оценки ситуации; они не требуют публичного рассказа. Ребёнок может обратиться к родителю, другому безопасному взрослому или специалисту, которому доверяет. Помощнику не следует требовать пересылки интимного материала, обвинять пострадавшего или наказывать за сам факт признания.

Спокойный порядок на каждый день

Для неожиданного сообщения задайте три вопроса: ожидал ли я этот материал, соответствует ли действие обещанию и могу ли я проверить автора отдельно? Неочевидный ответ - достаточная причина отложить открытие. Это правило подходит и для личной почты, и для школьного чата, и для рабочего мессенджера. Ограничивайте доступ приложений к контактам, камере и микрофону по реальной необходимости.

Если файл уже установлен или вы разрешили удалённый доступ, переходите к отдельной памятке. Связывайтесь с банком и поддержкой с безопасного другого устройства, когда есть риск наблюдения. Не пытайтесь исправить всё под руководством того же неизвестного человека. Учебная проверка в этом уроке не запускает настоящие файлы, не записывает голос и не просит прислать переписку.

Варианты для устройств

Установка вместо фотографии

1. Отмените неожиданную установку.
2. Не разрешайте обход ограниченных настроек ради присланного файла.
3. Проверьте происхождение приложения по официальной справке производителя.

Ограничения: Производитель и версия Android меняют предупреждения и разрешения.

Неожиданный запуск программы

1. Посмотрите полное имя и назначение файла без запуска.
2. Не выдавайте административные права неизвестному вложению.
3. Уточните безопасный формат у известного отправителя.

Выберите следующий шаг в переписке

1. Откройте учебную просьбу знакомого.
2. Найдите действие, которое требует отдельной проверки.
3. Выберите другой известный контакт.
4. Объясните, почему фото профиля и голос не заменяют проверку.

Проверьте себя

- Я проверяю необычную просьбу отдельно.
- Я не устанавливаю приложение вместо просмотра материала.
- Я понимаю, что видно при демонстрации экрана.
- Я могу обратиться за помощью при угрозах.

Практика: Что ответить «знакомому»?

Знакомый аккаунт просит перевести деньги. Выберите одно безопасное следующее действие.

Учебный пример. С аккаунта «Алексей, сосед» пришло: «Очень срочно одолжи 4 000 ₽, звонить не могу. Вот новая карта, потом всё объясню». Деньги в тренажёре не переводятся.

Какое действие сейчас лучше? Выберите один ответ.

- 1) Позвонить Алексею по ранее сохранённому номеру и проверить просьбу
- 2) Сначала отправить 100 ₽ для проверки
- 3) Попросить голосовое сообщение и довериться знакомому голосу
- 4) Позвонить по новому номеру из этого сообщения

Разбор вариантов

✓ Позвонить Алексею по ранее сохранённому номеру и проверить просьбу. Это независимый канал, выбранный вами. Если не удаётся связаться, перевод откладывают.

Сначала отправить 100 ₽ для проверки. Пробный перевод не подтверждает владельца аккаунта или получателя и уже создаёт реальную потерю денег.

Попросить голосовое сообщение и довериться знакомому голосу. Запись может быть украдена или подделана. Она не заменяет независимого звонка.

Позвонить по новому номеру из этого сообщения. Новый контакт указан тем же непроверенным собеседником, поэтому независимой проверки не получается.

Проверка по известному каналу важнее срочности. Если деньги уже отправлены, немедленно сообщите своему банку.

Самопроверка

Ответьте, затем сверьтесь с объяснениями. Несколько правильных ответов отмечены в условии. В PDF ответы приведены сразу после каждого вопроса.

1. Знакомый внезапно просит перевод в Telegram. Как проверить просьбу?

Выберите один вариант.

- 1) Спросить в том же чате, точно ли это он
- 2) Связаться по ранее известному другому контакту
- 3) Считать фотографию профиля достаточным доказательством

Ответ: 2.

1) При чужом доступе ответ даст тот же посторонний.

2) Независимая связь помогает проверить и личность, и саму просьбу.

3) Фото можно скопировать вместе с именем.

Сначала проверьте человека и просьбу вне подозрительного диалога.

2. Голос похож на родственника. Что это меняет?

Выберите один вариант.

- 1) Можно выполнять срочные просьбы без проверки
- 2) Это обязательно подделка
- 3) Просьбу всё равно нужно подтвердить независимым способом

Ответ: 3.

- 1) Похожий голос не подтверждает намерение и обстоятельства.
 - 2) Одного сходства недостаточно и для такого вывода.
 - 3) Запись, синтез и давление делают отдельную проверку полезной.
- Проверяйте действие и контакт, а не только узнаваемость голоса.

3. Файл «фотографии.apk» предлагают установить на Android. Что выбрать?

Выберите один вариант.

- 1) Не устанавливать и запросить фотографии обычным безопасным способом
- 2) Дать все разрешения для просмотра фото
- 3) Отключить защитные предупреждения

Ответ: 1.

- 1) APK предназначен для установки приложения, что не соответствует обещанию фотографий.
 - 2) Права приложения могут открыть больше данных, чем нужно.
 - 3) Предупреждения нельзя обходить по просьбе незнакомого отправителя.
- Сопоставляйте ожидаемый материал с фактическим действием системы.

4. Какие данные могут попасть постороннему при демонстрации экрана? Выберите все подходящие.

Выберите все подходящие варианты.

- 1) Текст уведомлений и одноразовые коды
- 2) Только картинка обоев
- 3) Финансовые сведения и документы в открытых окнах

Ответ: 1, 3.

1) Они могут появиться поверх открытого приложения.

2) Трансляция показывает изменяющийся экран, а не одну безопасную картинку.

3) На экране могут быть личные данные независимо от цели звонка.

Завершайте демонстрацию до работы с секретами и финансовыми приложениями.

5. Незнакомец угрожает публикацией личного материала. Какой первый выбор безопаснее?

Выберите один вариант.

- 1) Заплатить за обещание удалить
- 2) Прекратить выполнение требований и обратиться за помощью
- 3) Переслать материал всему классу для объяснения

Ответ: 2.

1) Оплата не гарантирует удаления и может вызвать новые требования.

2) Безопасный взрослый или другой доверенный человек помогает выбрать дальнейшие шаги.

3) Распространение увеличивает вред и нарушает приватность.

Помощь доступна без пересылки чувствительных материалов и без обвинения пострадавшего.

Продолжить обучение

- 10. Установил приложение или дал удалённый доступ
- 14. Знакомый просит деньги в переписке
- 16. Ребёнка запугивают или шантажируют

[Открыть урок на сайте](#)

ИСТОЧНИКИ И РЕДАКЦИОННЫЕ ОГРАНИЧЕНИЯ

Проверяйте по первоисточнику

Каналы, возможности и названия разделов могут изменяться. Материалы помогают выбрать действие, но не гарантируют восстановление аккаунта, возврат денег или отсутствие риска. При денежном происшествии обращайтесь в банк сразу.

1. Банк России. Вредоносные файлы под видом полезных материалов

https://www.cbr.ru/information_security/pmp/typical_fraudulent_schemes/27022026/

Содержание проверено · 2026-10-26 · Публикация: 2026-02-27

Официально описана рассылка вредоносных файлов, замаскированных под книги и программы.

Ограничения: Обобщённая схема без исследования конкретного устройства. Открытая ссылка, скачанный файл и установленная программа - разные события; заражение нельзя устанавливать заочно.

2. Уполномоченный при Президенте РФ по правам ребёнка. Звонки под видом сотрудников школы

<https://deti.gov.ru/Press-Centr/news/1771>

Содержание проверено · 2026-10-26 · Публикация: 2026-05-20

Описана схема со школьным предлогом, запросом SMS-кода и последующим запугиванием ребёнка.

Ограничения: Предупреждение, не индивидуальное происшествие. Не воспроизводим спорное обобщение о защите от перевыпуска SIM при помощи одного SIM-PIN.

3. Google. Ограниченные настройки Android

<https://support.google.com/android/answer/12623953?hl=en-ZZ>

Содержание проверено · 2026-10-26

Неожиданный контакт и просьба разрешить защищённые системой настройки рассматриваются как признаки риска.

Ограничения: Не всякая установленная вне магазина программа вредоносна; риск зависит от происхождения и фактических возможностей приложения.

4. МТС Банк. Важные правила защиты от мошенников

<https://www.mtsbank.ru/o-banke/novosti/detail/1150918/>

Содержание проверено · 2026-10-26 · Публикация: 2024-01-19

Просьбу знакомого о деньгах перепроверяют звонком; демонстрацию экрана и передачу банковских кодов прекращают.

Ограничения: Советы общего характера от банка; не подтверждают личность отправителя или безопасность отдельной операции.