Как защитить iPhone ребенка от мошенников

Мошенники не просто выманивают пароли. Они стали добиваться того, чтобы ребенок сам, добровольно выполнил на своем iPhone вход в чужой iCloud. После этого устройство блокируется злоумышленником, и требуется выкуп.

Как это происходит?

«Бесплатные игры и приложения»

Рекламируют доступ к играм («PUBG Mobile», «Standoff2») и модифицированного приложения «Telegram» в TikTok или Telegram. Ребенку в соцсетях или игровом чате новый «друг» предлагает установить мод, получить бонусы или «прокачать» персонажа. Для этого нужно «временно войти в его геймерский Apple ID» на своем устройстве.

Справочно:

моды — это дополнительные программы или файлы, которые создают сами игроки, чтобы изменить внешний вид персонажа или правила игры.

«Конкурс» или «Раздача призов»

Чтобы «получить приз», нужно подтвердить личность, войдя в предоставленный iCloud на своем устройстве. Мошенник утверждает, что это «временная процедура для проверки».

Объяснение ребенку: «Призы не требуют входа в чужие аккаунты. Это 100% обман».

Что происходит после входа в чужой iCloud?

Активируется функция «Найти». Как только в Настройках → [Имя] появляется чужой Apple ID, мошенник со своего устройства сразу видит iPhone ребенка в списке своих.

Устройство мгновенно блокируется. Мошенник дистанционно активирует «Режим пропажи» на iPhone. На экране появляется сообщение, что устройство утеряно и заблокировано.

Появляется требование выкупа. Приходит сообщение с контактом мошенника и требованием заплатить за разблокировку.

Ключевые правила для ребенка!

«ЧУЖОЙ Apple ID — НЕ ВВОДИ! НИКОГДА!». Ни при каких условиях, даже если просит друг.

Настройки iPhone — это не для игр. Нельзя выполнять в настройках телефона (раздел iCloud/Apple ID) то, что советует незнакомый человек из интернета.

«Бонусы» и «читы» — это обман. Настоящие моды и читы так не устанавливаются. Этого не существует.

Справочно:

читы — это программы или коды, которые дают игроку нечестное преимущество в видеоиграх. Например, позволяют видеть сквозь стены, стрелять без промаха или делать персонажа бессмертным.

Если уже начал диалог и просят зайти в Настройки — СТОП! Выключи устройство и расскажи родителям.

Что должны сделать родители: возьмите iPhone, откройте «Настройки» → [Имя] и покажите ребенку, как выглядит экран входа в Apple ID. Скажите: «Эту область трогать без меня нельзя».

Настройте «Семейный доступ». Организатор семьи может увидеть, если на устройстве ребенка вдруг появился новый аккаунт.

Важно: Для детского аккаунта в настройках «Семейного доступа» установите «Запрос на покупки». Это добавит еще один барьер.

Ограничьте возможность установки программ.

В «Экранном времени» → «Контент и конфиденциальность» можно запретить установку и удаление приложений без пароля. Это снизит риск, если обман связан со скачиванием приложения.

Что делать, если ребенок уже вошел в чужой iCloud и телефон заблокирован?

НЕ ПЛАТИТЕ! Выплата не гарантирует разблокировку. Вы потеряете деньги, и мошенник может потребовать еще.

Если блокировка уже случилась, следуйте строго инструкциям службы поддержки Apple.

Подготовьте чек/документ о покупке iPhone. Это главное доказательство того, что вы — владелец устройства. Без чека шансы на помощь резко падают.

Больше информации в телеграм-канале «КИБЕРКРЕПОСТЬ». Осуществить подписку на телеграм-канал можно с использованием QR-кода, а также путем введения в поисковую строку мессенджера «Telegram» «КИБЕРКРЕПОСТЬ».

Как не превратить iPhone в «кирпич»

Мошенники используют различные уловки, чтобы заблокировать ваше устройство, вынуждая войти в их учётную запись Apple (iCloud)

Основные схемы обмана

«Помощь с файлами»

Ссылаясь на «неисправное устройство», просят помощи в доступе к файлам (фотографиям, документам и т.д.) из облачного хранилища iCloud путем авторизации в мошеннической учётной записи

«Бесплатные игры и приложения»

Рекламируют доступ к играм («PUBG Mobile», «Standoff 2») и приложениям («AioGram») в TikTok или Telegram, предлагая установить их через предоставленный аккаунт Apple

«Работа/подработка»

Обещают вакансию (часто связанную с тестированием приложений), но требуют входа в "корпоративный" аккаунт Apple

Как защитить себя

- не сообщайте никому свои учётные данные (логин и пароль) от аккаунта Apple (iCloud)
- не входите на своём мобильном устройстве в аккаунт Apple (iCloud), предоставленный незнакомцами из Интернета
- не переходите по неизвестным ссылкам и не вводите данные Apple ID на посторонних сайтах

ВАЖНО!

Если ваш аккаунт заблокирован мошенником, сервисные центры не помогут. Разблокировка возможна только через официальную техподдержку Apple при наличии документов, подтверждающих покупку устройства.

БОЛЬШЕ ИНФОРМАЦИИ

В Telegram-канале
КИБЕРКРЕПОСТЬ
CYBER_FORTRESS_BREST

Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь