

Учителю пишет «директор»: как проверить подозрительное поручение

Памятка сотруднику

Применяйте её, когда «руководитель» в мессенджере или по телефону просит срочно перевести деньги, назвать код, прислать пароль, список или документы, сообщает о звонке «сотрудника» или требует никому не говорить. Проверка может занять время.

- Остановитесь. Коды и пароли не передаются в ответ на поручение никому, даже знакомому. Перевод денег и отправку служебных файлов отложите до проверки поручения по принятому в школе порядку.
- Позвоните сами по номеру директора или канцелярии, который знали раньше. Номер из сообщения и звонок в тот же чат не годятся: проверка через тот же подозрительный аккаунт не является независимой.
- Директор недоступен: обратитесь к известному заместителю или подойдите лично.
- Сохраните скриншоты, время и имя аккаунта в месте с ограниченным доступом, не в общей папке школы. Коды, пароли и данные детей не публикуйте.
- Сообщите проверенным каналом: директору, заместителю или [контакт для проверки]. Факты показывайте только ответственному.
- Имя, фото, голос и старая переписка личность не подтверждают. Настоящий аккаунт тоже может оказаться под чужим контролем.

Действия директора и что делать, если просьбу уже выполнили

Директор предупреждает коллектив через известный исправный канал, называет [контакт для проверки] и вместе с ответственным за ИТ определяет случай.

Отдельный аккаунт с вашим именем — возможный клон: сообщите о нём через сервис мессенджера. Сообщения из настоящего аккаунта, неизвестные сеансы или входы — подозрение на посторонний доступ, даже если вы ещё входите: чужие сеансы могут оставаться. ИТ помогает проверить сеансы, завершить чужие и восстановить доступ по официальной инструкции сервиса. Сотрудник не ведёт самостоятельное расследование.

- Передан код: восстановите доступ через официальный сервис с безопасного устройства, завершите незнакомые сеансы и, если применимо, смените пароль по официальной инструкции сервиса.
- Назван банковский код или переведены деньги: сразу позвоните в банк по официальному номеру.
- Если подозреваете мошенничество, обратитесь в полицию. Возврат денег заранее никто не гарантирует.
- Затронуты школьные данные: сообщите директору и ответственному за защиту данных. Ответственный оценивает инцидент, а также требуемые меры реагирования и уведомления. Смена пароля и эта памятка порядок реагирования не заменяют.
- Обращения и скриншоты храните в месте с ограниченным доступом.

Готовое сообщение для чата и источники

Перед отправкой замените [контакт для проверки] на должность, имя и заранее известный сотрудникам телефон. Для предупреждения используйте канал, доступ к которому проверен.

Коллеги, напоминаю правило проверки. Если вам пишет или звонит человек, который представляется директором или завучем, и просит срочно перевести деньги, назвать код, прислать пароль, список или документы, остановитесь и проверьте просьбу. Имя и фото в профиле легко скопировать. Коды и пароли не передаются в ответ на поручение никому, даже знакомому человеку. По деньгам и служебным файлам сначала позвоните руководителю сами по номеру, который знали раньше, или обратитесь к [контакт для проверки]. Скриншоты, время и имя аккаунта сохраните и покажите только [контакт для проверки]. Спросить можно в любой момент.

Источники: Банк России, схема с ложными аккаунтами руководителей: www.cbr.ru

Прокуратура РБ, восстановление Госуслуг и выход с других устройств (для других сервисов — по их официальной инструкции): epp.genproc.gov.ru