СХЕМА «ЦИФРОВОЙ ДВОЙНИК РУКОВОДИТЕЛЯ»

Легенда

В мессенджер поступает **сообщение от имени руководителя организации** (для этого злоумышленники делают «двойник» аккаунта руководителя),
в которой работает потенциальная жертва.
В сообщении **псевдоруководитель организации обращается с просьбой о помощи в решении проблемы или сообщает о проблемах самой жертвы.**

Возможные варианты легенды:

- **сбор средств с сотрудников** в целях временной помощи организации с обещанием последующего возврата денег с вознаграждением;
- утечка персональных данных работников и необходимость **помещения денег сотрудников на «безопасные» счета;**
- допущенная сотрудником (жертвой) ошибка, из-за которой **компания потерпела убытки** или **получила штраф** от контролирующих органов, который должна взять на себя жертва.

Цель звонка

Получение денежных средств от жертвы.

Механизм кражи денег

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. Мошенники используют ПСИХОЛОГИЧЕСКИЕ ПРИЁМЫ для управления действиями человека.

Что такое «цифровой двойник руководителя»?

ЭТО ВИРТУАЛЬНАЯ КОПИЯ РЕАЛЬНОГО РУКОВОДИТЕЛЯ, СОЗДАННАЯ НА ОСНОВЕ ЕГО ДАННЫХ, для взаимодействия в рабочих ситуациях. Но мошенники используют его как поддельный аккаунт руководителя в мессенджерах.

Признаки, что звонок исходит от мошенников

Руководитель связался с Вами не тем способом, как Вы обычно общаетесь, ведет беседу в несвойственном ему стиле.

Всегда требуют быстрого решения, не дают возможности обсудить проблему с близкими или коллегами.

Запрещают обсуждать разговор с кем-либо из коллег.

Настойчивы. Запугивают (если не оказать требуемую помощь, компания может обанкротиться или фонд оплаты труда попадет в руки мошенников).

Алгоритм действий

Подозрительные звонки нужно **НЕМЕДЛЕННО ПРЕРЫВАТЬ**, а полученную от собеседника **информацию перепроверить, обратившись к руководителю через привычный канал связи.**

Правила, которым нужно следовать, чтобы не стать жертвой мошенников

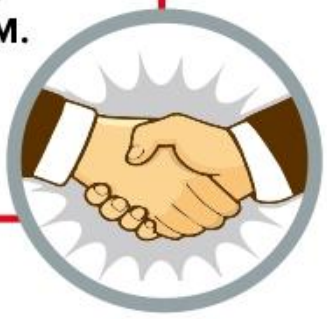
Помните, что РАБОТОДАТЕЛЬ НЕ МОЖЕТ ТРЕБОВАТЬ от сотрудников ПЕРЕВОДИТЬ СРЕДСТВА в качестве помощи организации или ВЫВОДИТЬ СРЕДСТВА на «безопасные» счета.

Правила, которым нужно следовать, чтобы не стать жертвой мошенников

НИКОГДА НЕ ПЕРЕДАВАЙТЕ
свои персональные сведения и коды подтверждения третьим лицам, даже если они представляются сотрудниками государственных учреждений или представителями компании-работодателя.

Важно!

Вы всегда **МОЖЕТЕ СВЯЗАТЬСЯ** с написавшим Вам руководителем иным ПРОВЕРЕННЫМ СПОСОБОМ. Если такой возможности нет, стоит задуматься, будет ли Вам лично писать руководитель, с которым нет прямой связи.



Больше информации на странице ФМЦ ФГН и на портале Моифинансы.рф

FINGRAM.REA.RU

МОИФИНАНСЫ.РФ