

Почему работники могут стать жертвами мошенников?

Авторитет начальника и доверие знакомому человеку. Большинство уже выработало иммунитет к просьбам «полицейских» или «следователей». В схеме с «начальником» все иначе — к жертве обращается якобы знакомый и влиятельный человек.

Переадресация на внешних исполнителей.

В примитивных вариантах схем «начальник» отдает распоряжение сам, но чаще он просит обсудить детали с сотрудником «ФСБ», «полиции» или «налоговой».

Большая срочность. Это важно, чтобы у жертвы не было времени подумать и разобрать ситуацию.

Абсолютная секретность. Чтобы никто не мог вмешаться в разыгрываемую сцену, «босс» предупреждает жертву, что обсуждать происшествие ни с кем нельзя.



Каковы цели атаки?

- Если жертва уполномочена проводить в фирме финансовые транзакции, ее будут убеждать провести срочный «секретный платеж» или перевести деньги на «безопасный» счет.
- Для сотрудников, не связанных с финансами, целью атаки будут либо данные компании — например, пароли к внутренним системам, — либо их собственные средства.
- Для большей убедительности мошенники могут пообещать компенсировать все расходы и труды жертвы — потом.



Важны ли детали?

- Благодаря многочисленным утечкам данных и публикациям в соцсетях, мошенникам стало проще проводить персонализированные атаки.
- Они могут заранее уточнить полное имя жертвы, ее руководителя, директора фирмы, узнать имена реальных сотрудников.
- Если на кону стоят серьезные суммы, мошенники могут провести длительную подготовку, чтобы разыгранная ими схема была предельно убедительна.



Технические аспекты

- Сложные мошеннические схемы почти всегда включают в себя общение со злоумышленниками по телефону.
- Первичное сообщение «от босса» может поступать разными способами — в рабочей электронной почте, мессенджере или опять же по телефону.
- Что касается телефонных звонков, то злоумышленники часто используют специальные сервисы, позволяющие подменять номер, или нелегально получают дубликат сим-карты.
- Во время звонков злоумышленники могут пользоваться инструментами автоматической замены голоса.



Как защититься от мошенников?

Не торопитесь и не паникуйте. Задача мошенников — вывести вас из равновесия. Сохраняйте спокойствие и перепроверьте все факты.

Обращайте внимание на адрес, телефон и аккаунт отправителя. Если вы обычно переписываетесь с начальником по почте, а тут он вдруг отправляет вам сообщение в мессенджере с незнакомого номера — время насторожиться.

Следите за нюансами. Странные просьбы, необычные формулировки и речевые обороты, грамматические ошибки и нетипичное оформление документов — проанализируйте все эти «красные флаги».

Насторожитесь при необычных требованиях. Если начальник или коллега требует срочно сделать что-то нестандартное, да еще сохраняя это в тайне, то это почти всегда признак мошенничества.

Уточните информацию у других коллег и обратитесь в правоохранительные органы или в службу безопасности компании.