

Социальная инженерия в условиях цифровой трансформации: от фишинга к манипуляции доверием

Долгое время социальная инженерия воспринималась как набор примитивных приёмов: поддельное письмо, звонок от «службы безопасности», просьба сообщить пароль. Сегодня ситуация изменилась. Цифровая трансформация расширила не только количество каналов коммуникации, но и возможности для манипуляции. Злоумышленник уже не просто имитирует отправителя, он выстраивает доверие, использует контекст, играет на привычках и эмоциях. В результате традиционные рекомендации «не открывать подозрительные письма» перестают работать. Современная атака всё чаще начинается не с технической уязвимости, а с человека. Исследования показывают, что большинство успешных проникновений в корпоративные системы связано именно с человеческим фактором. При этом цифровая среда создаёт благоприятные условия: сотрудники работают в мессенджерах, социальных сетях и на множестве платформ, а границы между личным и рабочим общением размываются. Злоумышленник может собрать информацию о человеке из открытых источников, определить его интересы, круг общения и привычный стиль коммуникации.

Доцент кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.э.н., доцент Рожков Р.С. отмечает, что особую роль играет доверие к каналу. Если сообщение приходит в привычном мессенджере, от знакомого контакта или в рамках рабочей переписки, критичность восприятия снижается. Злоумышленники используют это: компрометируют учётные записи, создают поддельные профили, имитируют стиль общения руководителей и коллег. Модели ИИ позволяют делать такие сообщения персонализированными и естественными, а синтез голоса и изображения позволяют дополнять их убедительными аудио- и видеоматериалами.

Отдельное направление – это манипуляция через контекст. Атака может быть привязана к реальному событию: сделке, командировке, отчётному периоду, кадровым изменениям. Злоумышленник использует срочность, авторитет или страх ошибки. Например, сотруднику сообщают о «проверке», «утечке» или «срочном поручении руководителя» и требуют немедленных действий. В состоянии стресса или спешки человек реже проверяет информацию и легче подчиняется инструкциям.

Цифровая трансформация добавила новую возможность атаки на корпоративные системы коммуникации. Мессенджеры, платформы совместной работы, системы электронного документооборота и видеоконференцсвязи становятся каналами, через которые злоумышленник может взаимодействовать с сотрудниками напрямую. Если доступ к такой системе скомпрометирован, атакующий может действовать от имени коллеги, не вызывая подозрений.

По мнению доцента кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.э.н., доцента Данилиной М.В., противодействие социальной инженерии требует комплексного подхода. Такие технические средства как фильтрация, многофакторная аутентификация, мониторинг аномалий, необходимы, но недостаточны. Важна культура безопасности: сотрудник должен понимать, что убедительное сообщение, знакомый голос или видеозвонок не являются достаточным основанием для доверия. Критические действия, такие как перевод средств, передача данных, изменение реквизитов, должны подтверждаться независимым каналом связи.

Таким образом, социальная инженерия перестала быть набором технических приёмов и превратилась в системную угрозу, использующую доверие как основной инструмент. Цифровая трансформация расширила возможности злоумышленников, но одновременно дала организациям понимание: защита начинается не с технологии, а с человека. Именно поэтому обучение, проверка и культура безопасности становятся не менее важными, чем программные и аппаратные средства защиты.

Рожков Р.С.,

кандидат экономических наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ

Данилина М.В.

кандидат экономических наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ