# Более 200 почтовых доменов могут быть использованы для кибератак на ТЭК

*Доля целевых атак на крупнейшие компании нефтегазового сектора в первом полугодии 2026 года выросла вдвое, с 5 до 11%. Одной из угроз стали атаки типа ghost invoice — схемы с использованием подмены платежных реквизитов.*

С начала 2026 года эксперты BI.ZONE Digital Risk Protection выявили свыше 1,1 тыс. зарегистрированных доменов, в названиях которых присутствовало упоминание нефтегазовой компании. У 20% из них уже была настроена электронная почта, что позволяет мошенникам использовать домены, похожие на официальные, для полноценной переписки.

Существует несколько сценариев мошенничества с поддельными счетами. Первый — создание доменов-двойников, отличающихся от оригинальных одним или парой символов. В этом случае мошенники вступают в переписку от имени контрагента и предоставляют собственные реквизиты. Второй сценарий предполагает компрометацию существующей переписки, например через инсайдеров или взлом почты: изучив контекст сделки, злоумышленники внедряются в диалог в момент согласования платежа и направляют жертве поддельные документы на оплату.

Если раньше атаки строились на массовой рассылке предложений потенциальным клиентам компании, то сегодня злоумышленники используют более сложную схему: они имитируют тендерные площадки и заманивают жертв ложным выигрышем в закрытых закупках, вынуждая их таким образом обходить стандартные процессы. По данным BI.ZONE Mail Security, за первое полугодие было выявлено около 80,2 тыс. уникальных писем на тему тендеров и закупок, из которых 2,3 тыс. (2,9%) оказались фишинговыми. Более половины мошеннических писем маскировались под юридическое сопровождение тендеров по Федеральным законам № 44-ФЗ и № 223-ФЗ. Еще около 30% имитировали приглашения к закупкам от имени конкретных компаний, используя названия потенциальных заказчиков как приманку.

**Дмитрий Кирюшкин, руководитель BI.ZONE Digital Risk Protection:**

> *Топливно-энергетические организации входят в топ-3 популярных мишеней для атак типа ghost invoice. Интерес обусловлен спецификой бизнеса и крупными бюджетами. Сложные разветвленные цепочки поставок, высокие средние чеки транзакций, а также чувствительные данные в договорах привлекают киберпреступников. Кража суммы лишь одного платежа может*

*привести к масштабному финансовому и репутационному ущербу компании.*

ТЭК находится под давлением сразу двух типов угроз: как массовых мошеннических атак, так и целевых. По данным BI.ZONE Threat Intelligence, доля целевых атак на компании промышленного комплекса растет: если в 2025 году она составляла 5–6%, то в первом полугодии 2026-го достигла 11%.

Защитой от подобных типов атак служат не только технические средства защиты, но и организационные меры. Помимо обязательной проверки адресов отправителей и ссылок на электронные торговые площадки (ЭТП), компаниям следует обращать внимание на аномалии в документации, таким как, например, отказ от банковских гарантий. Ключевым правилом безопасности остается верификация контактов: при любых подозрениях необходимо связываться с контрагентом только по проверенным официальным контактам, найденным в независимых источниках.

---