Почти четверть сотрудников российских компаний создают риски утечек информации

Эксперты узнали, какие уязвимости появляются в российских компаниях из-за недобросовестных работников

Каждый десятый сотрудник российских компаний использует слабые пароли для своих рабочих аккаунтов, что создаёт серьёзные риски для информационной безопасности. Также распространены другие угрозы: 5% сотрудников сталкиваются с утечкой данных из-за фишинговых атак и передают конфиденциальную информацию через незащищённые каналы, включая популярные мессенджеры, такие как WhatsApp. Проблемой является также использование рабочих устройств не по назначению — об этом сообщает 4% сотрудников. В целом, 76% работников компании придерживаются правил безопасности, минимизируя риски.

По словам экспертов, такие ошибки сотрудников могут привести к серьёзным последствиям для компаний. Например, утечка данных или открытие доступа к корпоративной сети может закончиться штрафами, кражей информации, шифрованием данных или даже вымогательством. Ситуация усугубляется, когда работники игнорируют базовые правила безопасности, создавая благоприятные условия для киберпреступников.

Для минимизации таких рисков специалисты советуют усилить осведомлённость сотрудников и проводить регулярные тренинги. Виктор Иевлев, руководитель отдела информационной безопасности группы компаний «Гарда», подчеркнул, что повышение уровня знаний сотрудников в области информационной безопасности — это один из самых эффективных способов защиты от киберугроз.