В интернете стали появляться новые сценарии целевого фишинга, направленные на сотрудников компаний, предупреждают эксперты. Злоумышленники выдаёт себя за специалистов технической поддержки и отправляют работникам вредоносные электронные письма, целью которых является получение доступа к их паролям и конфиденциальным данным.

Эксперты из компании R-Vision сообщают, что в интернете наблюдается тенденция злоумышленников, которые под видом сотрудников служб технической поддержки различных организаций проводят атаки. Они используют два основных метода: в первом случае отправляют письмо с уведомлением о смене внутреннего доменного адреса. В письме указывается, что сотрудники должны перейти по ссылке на новый адрес и проверить доступ к своим проектам, используя корпоративные пароли.

Другой распространённый метод — фишинговые письма, выглядящие как уведомления о тестировании нового алгоритма шифрования при работе с почтой. Мошенники персонализируют сообщения, адресуя их конкретным сотрудникам, и ведут себя от имени реальных сервисов, используемых в компании. Если сотрудник переходит по ссылке и вводит учётные данные, злоумышленники получают доступ к его персональной информации и паролям, что может привести к серьёзным последствиям.

Такие атаки от имени техподдержки были известны и ранее, но сейчас они снова актуальны из-за своей эффективности и распространённости среди преступников. Специалисты рекомендуют всегда быть бдительными при получении подобных сообщений, проверять их на подлинность и никогда не вводить конфиденциальные данные, не убедившись в их истинности.