Уважаемый поставщик,

Социальная инженерия остается одной из крупнейших финансовых угроз, с которыми сегодня сталкиваются организации. Мошенники заметно активизируются в течение напряженных сезонов, мы ожидаем увеличения попыток социальной инженерии в течение предстоящих праздников.

Поэтому мы хотели бы указать на схему социальной инженерии, которую мошенники пытались использовать в последнее время:

Мошенники создают доменные имена, которые выглядят как настоящие домены METRO, например, ***metro-group.biz, metroholding.de, metro-groupes.fr*** *и т. д., чтобы выдавать себя за METRO при общении с третьими лицами. Например, они размещают заказы у поставщиков, используя 30-дневные условия оплаты, и получают товары, даже не оплачивая их, потому что поставщики считают, что имеют дело с METRO, и добросовестно осуществляют доставку.*

Нам известно, что этот вид мошенничества может нанести значительный финансовый ущерб нашим поставщикам и деловым партнерам, поэтому мы обращаем Ваше внимание на эту схему.

Эта практика используется мошенниками не только с использованием названия компании METRO, но и с именами и брендами многих других известных компаний.

Если Вы не уверены, является ли электронное письмо подлинным, мы рекомендуем дважды проверить домен, используемый его отправителем, и личность отправителя через канал связи, отличающийся от предложенного в подозрительном сообщении (например, прямой звонок Вашему категорийному менеджеру). Если Вы обнаружите, что электронное письмо не было отправлено подлинным источником METRO, пожалуйста, игнорируйте это электронное письмо и не отвечайте на любые дальнейшие попытки связи его отправителем. Свяжитесь с Вашим категорийным менеджером в METRO и сообщите о случившемся.

Если у вас есть какие-либо дополнительные вопросы, пожалуйста, свяжитесь с Вашим категорийным менеджером.