



Бизнес без риска

Как пытаются увести
кабельную продукцию
на миллионы рублей
через домен **maxsidom.ru**
и «закупочную площадку»

— 08

Разбор фишинговой схемы,
в которой неустановленное лицо
имитирует закупочную деятельность
крупного ритейлера, чтобы получить
продукцию без оплаты



МаксидоМ



Суть схемы

1

Регистрация домена-клона с опечаткой (тайпсквоттинг) maxsidom.ru который визуально почти не отличим от официального домена крупной сети гипермаркетов «Максидом»



2

Развертывание «технических» доменов под видом B2B-площадок с вариациями в наименованиях market, zakupki, b2b, tender и др. для реализации легенды площадки-посредника между поставщиком и «заказчиком»



3

Создание образа заказчика, которому можно верить. Изготовление поддельных корпоративных документов (приказы, уведомления, карточка предприятия) с реальными реквизитами и ФИО из открытых источников



4

Фишинговая рассылка с имитацией срочной закупочной процедуры кабельной продукции для внутренних нужд с рыночной стоимостью на десятки млн. руб.



5

При ответе жертвы запускается социальный сценарий, в результате которого мошенники убеждают жертву передать товар без оплаты (с отсрочкой платежа) по поддельным документам



6

Хищение, которому способствует схема логистики - «самовывоз или доставка до склада (по согласованию)», т.е. адрес выгрузки водитель узнаёт уже после погрузки, поэтому перехватить ТМЦ физически крайне сложно. Далее реализация на теневом рынке или сдача кабеля как лома, связь обрывается





Как понять, что перед вами фишинг, а не реальная закупка

Домен не тот

maxsidom.ru вместо официального — тайпсквоттинг

«Технические» домены
в переписке

Слова market, zakupki, b2b, tender в адресе отправителя

Разные домены
«от» и «кому»

Письмо с «торговой площадки», а ответ на домен-клон

«Прямая закупка
в обход портала»

Любые формулировки про «внутренние нужды»,
«разовую сделку», «срочно, мимо общей процедуры»

Нет ЭДО и УКЭП

Только сканы или «оригиналы» (через курьера),
только «синие» печати и подписи

Крупная сумма, отсрочка,
нет аванса

Новый контрагент, стоимость товара на млн. руб.,
отсрочка без аванса

Нет точного адреса выгрузки

«Доставка до склада», «по согласованию»,
«самовывоз» — адрес сообщается постфактум

Жёсткий дедлайн по КП

Короткий срок ответа





Рекомендации для бизнеса



**Заблокировать
выявленные домены
и IP-адреса мошенников
в системах безопасности
предприятия**



**Верифицировать
любые запросы только
через официальные
контакты заказчика
(не по контактам
из письма)**



**Запретить отсрочку
по новым запросам
от непроверенных
контрагентов**



**Проверять
документы на маркеры
подделки**



**Письма, где «отправитель»
и «получатель» на разных
доменах квалифицировать
как подозрительные
по умолчанию**



**Регулярно обучать
персонал распознаванию
признаков
фишинга**





Правовое ограничение



- Данный материал носит аналитический характер и не является итоговым юридическим заключением.
- Выявленные признаки носят вероятностный характер и требуют процессуальной проверки.
- Окончательная квалификация действий осуществляется исключительно правоохранительными органами и судом.
- Организация считается добросовестной до вступления в силу обвинительного приговора.



**ЧЕСТНАЯ
ПОЗИЦИЯ**

АССОЦИАЦИЯ
ДИСТРИБЬЮТОРОВ
И ПРОИЗВОДИТЕЛЕЙ
ЭЛЕКТРОТЕХНИКИ



Бизнес без риска

Выявление мошеннических схем,
пресечение противоправных действий,
защита интересов и обеспечение
безопасности добросовестных
участников электротехнического рынка

fairp.ru



Выявление
фактов
мошеннических
действий



Раскрытие
преступных схем
и информирование
рынка



Реализация
комплекса
превентивных
мер



Оказание
помощи
участникам
рынка



Взаимодействие
с государственными
органами



Аналитика
и ведение
реестра

