Один из методов борьбы со спамом

02.06.2025 23:25:50

Печать статьи FAQ

Категория:	Общие	**Голоса:**	0
Состояние:	общедоступное (всем)	**Результат:**	0.00 %
Язык:	ru	**Последнее обновление:**	18:16:35, Втр 21 Янв, 2025 г.

Ключевые слова

спам, почта, email

Симптомы (общедоступное)

Спам

Проблема (общедоступное)

Спам

Решение (общедоступное)

Сверяем домен из технического заголовка From с доменом из поля Reply-To.
Оригинал: https://www.kaspersky.ru/blog/from-reply-to-check/37982/
Чем помогает сравнение заголовков From и Reply-To

Большая часть атакующих, даже вклиниваясь в легитимную деловую переписку, особенно не утруждает себя взломом легитимных доменов, а надеется на, так сказать, ограниченную компетентность администраторов почтовых серверов. По факту у огромного количества доменов механизмы почтовой аутентификации типа Sender Policy Framework (SPF), и тем более Domain-based Message Authentication, Reporting and Conformance (DMARC), если и работают, то из рук вон плохо.

В лучшем случае они формально включены, но во избежание ложных срабатываний политики настроены настолько свободно, что ничем помочь не могут.

Поэтому злоумышленники (иногда даже стоящие за полноценными APT-атаками) просто берут домен атакуемой организации и ставят его в поле From или даже SMTP From. Однако поскольку при этом им нужно не просто доставить вредоносное письмо, но и получить на него прямой ответ, то в поле Reply-To они вынуждены поставить свой адрес. Обычно это какой-нибудь одноразовый почтовый ящик или адрес, расположенный на бесплатном почтовом сервисе. Что их и выдает.

[1]

Благодаря настройке [2]DMARC владельцы доменов могут создавать правила обработки писем, которые поступили с доменов, не прошедших авторизацию и проверять совпадают ли заголовки друг с другом (например, поля From: и Reply-to:).

[1] https://media.kasperskydaily.com/wp-content/uploads/sites/90/2024/07/25205851/from-reply-to-check-headers.jpg
[2] https://ru.wikipedia.org/wiki/DMARC