Email: Настройка собственного from-домена

Настройка SPF

Sender Policy Framework (SPF) - технология, позволяющая проверить не подделан ли домен отправителя. Для её работы необходимо добавить на отправляющий домен (сендер домен, фром домен) специальную TXT-запись, которая определяет политику разрешения отправки этого домена с различных хостов.

Мы рекомендуем внести записи разных версий:

Домен	Тип записи	Содержимое
example.com.	TXT	v=spf1 include:spf.aksend.net -all
example.com.	TXT	spf2.0/pra include:spf.aksend.net -all

На домене spf.aksend.net содержится актуальный список IP адресов сендеров Altcraft.

Если ваш фром домен уже используется для рассылок, то уточните, какие SPF-записи уже существуют и добавьте к ним "include:spf.aksend.net".

Важно! Обратите внимание на то, что мы рекомендуем использовать правило, запрещающее отправку с ресурсов, не перечисленных в SPF.

Настройка DKIM

Технология DomainKeys Identified Mail (DKIM) добавляет в письмо цифровую подпись, связанную с from-доменом. Подпись автоматически проверяется на стороне получателя, после чего используется для уточнения репутации и помечается для пользователя. Для подписи письма используется приватный ключ, который устанавливается на стороне отправщика и более никому не известен. Публичный ключ располагается в виде специальной TXT-записи на поддомене from-домена.

Необходимо внести следующие записи (используется ключ Altcraft, ak):

Домен	Тип записи	Пример содержимого
ak._domainkey.example.com.	TXT	v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCldFYh3Rfrmeov+WqYYpwfW2bVUzxXPy9dSVoUCGLKCn+vgY/pdKIIBFitkvZJXGLnHqreqwGzoriEWf9ZRd+cL2LdA4UrDKheMeorBd2NSIqihkTaKz8PA+SIBFxFGm2Z0Krh5ZDF2NtFVhtD4YvqmrFqk2muzZ0tFEko8zP30wIDAQAB
_domainkey.example.com.	TXT	o=-;

Настройка DMARC

Технология DMARC позволяет почтовому серверу решить, что делать с почтой, если с DKIM и SPF-записями что-то не так.

Мы рекомендуем установить правила, запрещающие принимать сообщения, которые получены с чужих IP-адресов, либо не правильно подписаны.

Домен	Тип записи	Пример содержимого
_dmarc.example.com.	TXT	v=DMARC1; p=reject; sp=reject; mailto:report@example.com

Настройка BIMI

Технология BIMI (Brand Indicators for Message Identification) используется совместно с SPF, DKIM и DMARC и используется для идентификации компании по брендовому изображению, помещаемому рядом с темой сообщения в инбоксе получателя. Почтовые провайдеры таким образом могут дополнительно валидировать отправителя.

> Аутентификацию писем BIMI поддерживают такие почтовые сервисы как Fastmail, Gmail, and Yahoo!

Чтобы использовать технологию, вам нужно указать путь до файла в формате **svg**. Изображение должно быть квадратным и не иметь дополнительных слоёв.

Внесите в настройках домена следующую запись:

Домен	Тип записи	Пример содержимого
default._bimi.example.com	TXT	v=BIMI1; l=https://example.com/bimi/bimi.svg

Вы можете также воспользоваться генератором записи на https://bimigroup.org/bimi-generator/

Настройка трекинга

На поддомене вашего фром домена необходимо внести следующую запись:

Домен	Тип записи	Пример содержимого
trk.example.com.	CNAME	trk.aksend.net

Дополнительно, вы можете использовать сколько угодно трекинг доменов, настройки будут аналогичные.