Чек-лист: что делать, если от вашего имени отправляют мошенники?

- Узнав о покушении на репутацию компании, остановите все реальные рассылки до тех пор, пока не перестанут отправляться поддельные письма.

- Проверьте, все ли необходимые DNS-настройки прописаны на вашей стороне: SPF-запись, DKIM-ключ, DMARC. Это можно сделать с помощью сервиса DNS Watch. Лучше, если SPF будет завершаться на «–all»: эта настройка пометит все емейлы с неразрешенных IP-адресов как «провалившие» проверку (SPF=fail). Такие письма привлекут внимание почтовых провайдеров и, вероятнее всего, скоро окажутся в спаме.

- Если вы ещё не внедрили политику DMARC, самое время это сделать. Чем строже она будет, тем меньше шансов у мошенников. Совсем скоро DMARC станет обязательным элементом DNS-настроек для российских отправителей. Поэтому, если вы ещё не знакомы с политикой, самое время подробнее почитать об этой технологии в нашей более ранней статье.

- Настройка DMARC обычно занимает время. Чтобы остановить мошенников как можно скорее, напишите в техподдержку почтовых провайдеров и попросите заблокировать отправки с домена до решения проблемы.

- Если в этом есть необходимость, расскажите своим подписчикам о фишинге и посоветуйте, как отличить настоящие письма компании от спама. Это будет честно и поможет сохранить репутацию. Если вы - крупная компания с миллионами клиентов, есть смысл обратиться в СМИ. Так вы, возможно, спасёте сбережения людей, которые поверят обманщикам, и восстановите их доверие.