WHAT IS THE PURPOSE OF THE SPF DKIM AND DMARC RECORDS?

SPF DKIM and DMARC are simply a set of email authentication methods to prove to ISPs and mail services that senders are truly authorized to send email from a particular domain and, are a way of verifying your email sending server is sending emails through your domain.

Steps to creating SPF/DKIM/DMarc records for campaigns

1. Every campaign will require SPF, DKIM and Dmarc records to be added to clients site.
2. This requires a representative from the client side that has access to the backend of website and hosting. In many cases, this might even be a third party if Pixa does not already handle the clients website hosting.
3. This process should start during the Production/Programming Step 5. It does take some time from client side and for the marketing automation platform to validate all information. Therefore, the sooner the better so there are no delays in campaign execution.
4. This information can be obtained from the programmer assigned to the campaign. You will make the request and then forward to the client.

Below are some samples that you will receive from programmer to pass onto client. If the client does not have a point person, we can walk them through the process. In some cases, if we are given access our team can implement.

SAMPLE #1

Step 1. Create the following DNS entry for the host name pixa._domainkey.hu-friedy.com

v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3d9X2wsLyFVzHhPAccWqRq0yoqwQ3PSGFhEc
GcEcD/oRyWBdJqWopMozqXTbBy6N2MrPCoRxyYj2nTAqQZLCZuGLz0QFkWy5YXOxJ3egocEpK7UsHk68V
TGPEI3xwC54jn/FfgJZpv/SeQwlSwHMU4b984Ho6pV8nOQSlRFWENQIDAQAB

Step 2. Edit your SPF record as such:

v=spf1 mx ip4:70.225.226.0/24 ip4:108.171.169.211/32 ip4:52.4.245.122/32 include:aspmx.pardot.com include:spf.protection.outlook.com include:musvc.com include:spf-003bcb01.pphosted.com include:_spf.salesforce.com include:email-od.com ~all

Step 3. Notify ray@thinkpixa.com when the two steps above have been completed.

Step 4. Pat yourself on the back for a job well done!

SAMPLE #2

Create the following records in your DNS zone file. Adding these records will tell requesting servers that you are allowing us to send emails on your behalf from a third party server.

Type: TXT
Host: 7bridges._domainkey.caseusa.com
Value: “v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKdbhD1R7KJClquwjxNDUr5xpXKmTnkuFq1KqZ
TkMXU4mvYg7fUVkyEHUZfwA2KMFd+durQ1HzzAGQ
+/XGdtkPSMZrtSvZPK6ea9DrlhATF3xlLkpkspLxCW1ydFKjWrxiJDfhpxccbp5+vzp8p/tdbz+edq56
+XhdfLEMGq5qqQIDAQAB”

Type: TXT
Host: @
Value: v=spf1 include:email-od.com ~all
*Note: Your domain may already have a SPF record. If so, you will simply include email-od.com in the current record.

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDKdbhD1R7KJClquwjxNDUr5xpXKmTnkuFq1KqZTkMXU4mvYg7f
UVkyEHUZfwA2KMFd+durQ1HzzAGQ+/XGdtkPSMZrtSvZPK6ea9DrlhATF3xlLkpk
spLxCW1ydFKjWrxiJDfhpxccbp5+vzp8p/tdbz+edq56+XhdfLEMGq5qqQIDAQAB
AoGAeze2E6KLgJ8NjeWTBamuiq+2OkKU8tNT2b7grTkSYAn5jAHz5zoNPQkDG6dN
q6iWNumwJcVtBSGt+l0+MbF3XF7OZnG7SXcW+Fw8eGryk9BVUZPX8aiGvJ1GTVx1
Bw+8nou+rlCQHGopF4pWntetjmlo8W5w0MExCE6l9zEfpZkCQQDeQQ2jXfIX+qFX
To3m1nH0NpkHKH9yt5twKjjKJ49U/8Gwxh8ZCQGEhm8g25hiTjGINDS7y1noUMBU
Gga9ygX/AkEA6TNE/GuXuJPmkeD677WwrVKlwE01lzHBei3pldHd9nAKuQLC+72w
xFhCOV8Tn9nUNjxGx6u+la5WSjHBELOfVwJBAJOwqv1qilvA4sH/o3BIBIWCWoJV
OQvkUthgVkiPrUGQiweLQFMElwuXwfUVt9drmrXrUTeR0/b64jOA8AXiX8UCQCeB
Feik2VjdRSvlLt04rCtQWt/OtIteVGY8LNvCZ5V9uXNJ8nnu0mkQgndxkcN8hSSC
5YKhp3F3zQpYj1oi85UCQQCE0Lr6IjqIbYvEdq9b60+eNunCZfqcdP0pzzfrgF7i
Baon1j/DdyTdM9i+HLS6KEt/eeWpQ12VpCCJ2pEqMsFH
-----END RSA PRIVATE KEY-----
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKdbhD1R7KJClquwjxNDUr5xpXKmTnkuFq1KqZ
TkMXU4mvYg7fUVkyEHUZfwA2KMFd+durQ1HzzAGQ
+/XGdtkPSMZrtSvZPK6ea9DrlhATF3xlLkpkspLxCW1ydFKjWrxiJDfhpxccbp5+vzp8p/tdbz+edq56
+XhdfLEMGq5qqQIDAQAB”