Office365 Basic Hygiene Checkup

This brief course covers some "basic hygiene" steps you can take to optimally secure your Office365 tenancy, in leui of Microsoft's "Advanced Threat Protection" service (*which can be costly as the volume of mailboxes scales out*).

SPF

What is it?

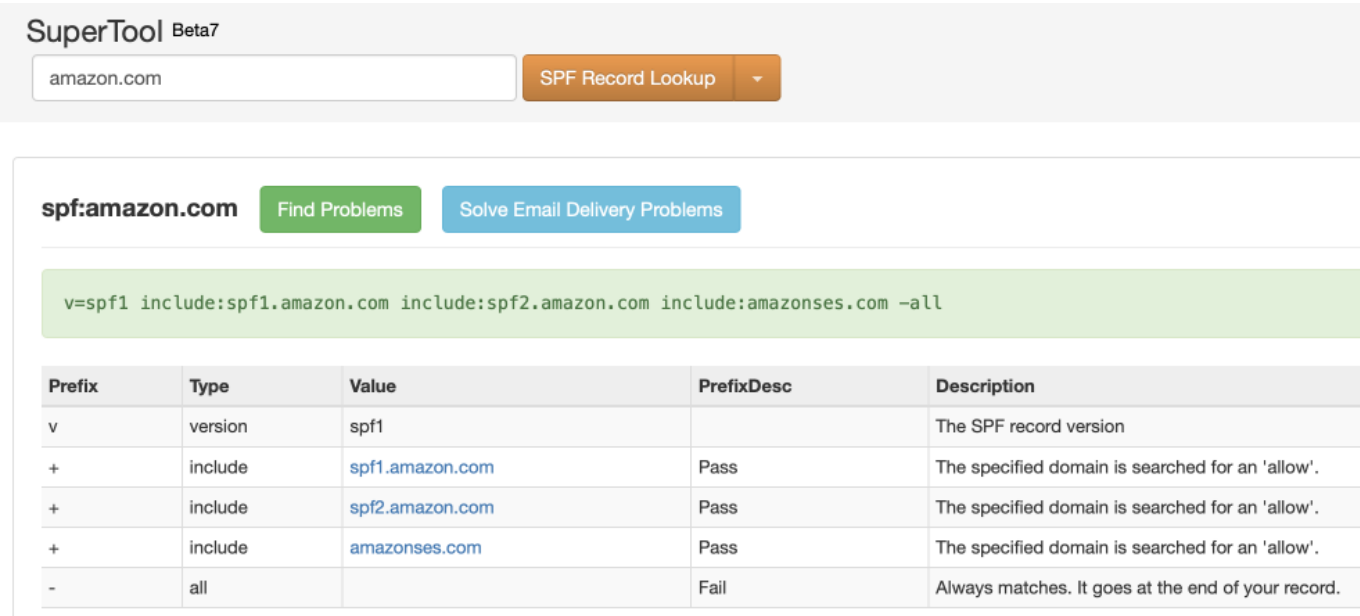
Sender Protection Framework (SPF) is a way to tell the rest of the world which servers are authorized to send email form your domain. (*For example, if your domain is hosted with Office365, recipients should discard any emails delivered from spammersrus.com purporting to be sent from your domain!*)

Do I have it?

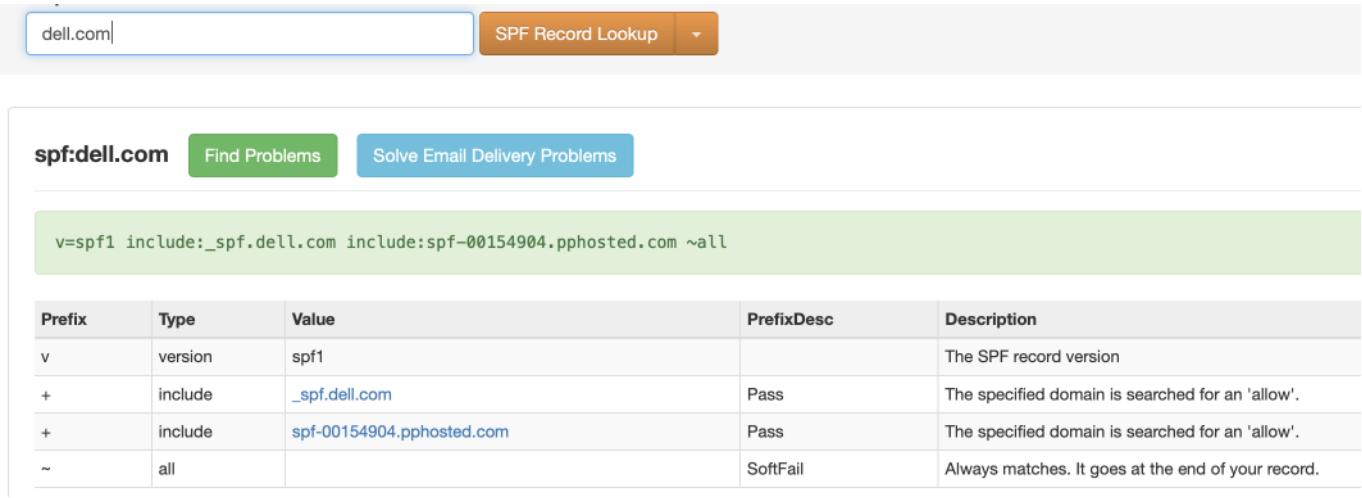
Enter your domain name into an online SPF testing tool (https://mxtoolbox.com/spf.aspx, for example). For maximum hygine, confirm that:

1. An SPF record exists for your domain
2. The SPF record ends in `-all` (A "hard fail", which instructs receiving mailservers that you do **not** authorize any senders other than those specified, for your domain)

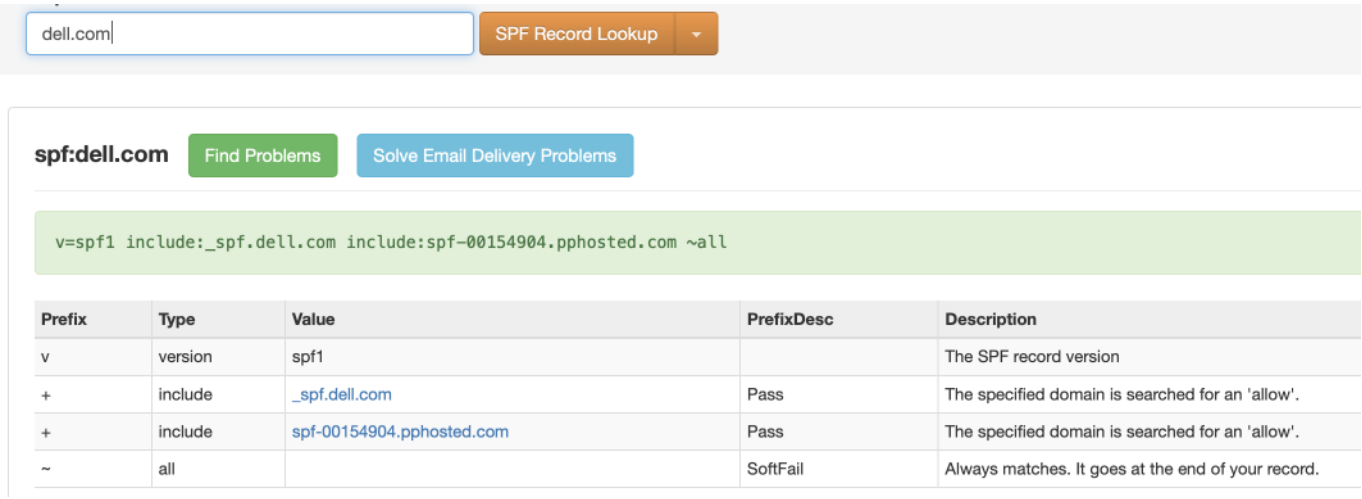
Here's an example of a well-defined SPF record, which hard-fails any unauthorized sources:



Here's an SPF record which, while defined, only soft-fails unauthorized sources (*leaving it up to the receiving mailserver to "make a judgement call"*):



And **here's** an example of a domain with no SPF record:



How do I get it?

You'll need access to administer your domain's DNS, and you'll want to create a DNS TXT record with the necessary SPF data. Microsoft's support docs explain the process in detail. There are many online SPF record generators, one notable one is https://mxtoolbox.com/SPFRecordGenerator.aspx. If you're fully hosted on Office365, for example, your SPF record could be as simple as `v=spf1 include:spf.protection.outlook.com -all`.

DKIM

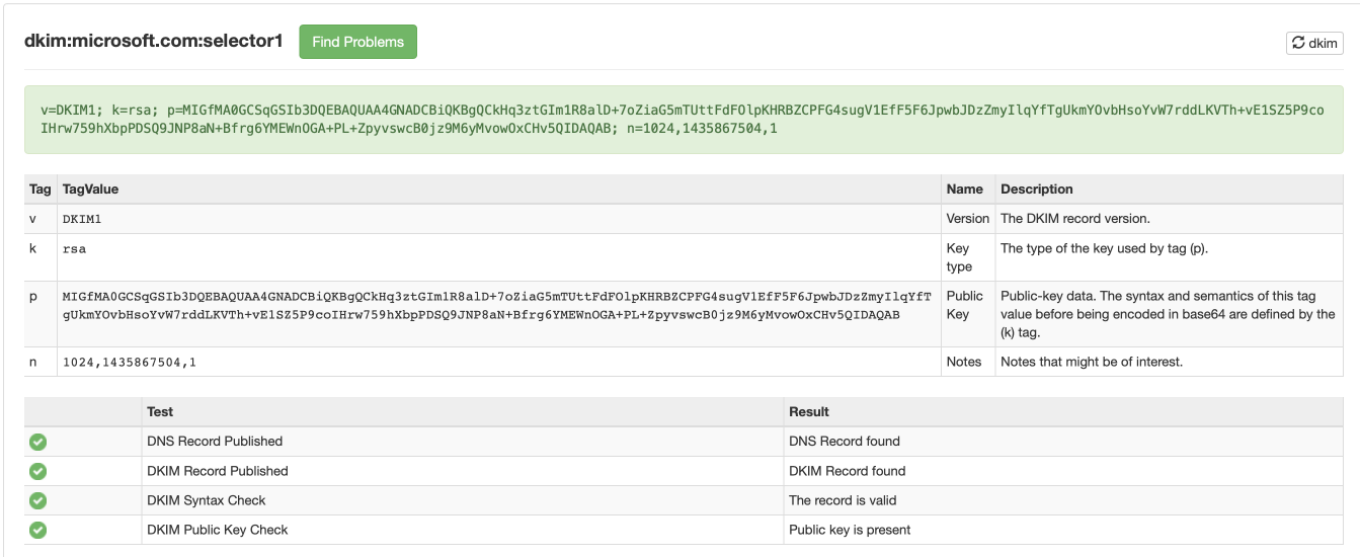
What is it?

DomainKeys Identified Mail (DKIM) is another strategy used to prove to the world which servers **should** be allowed to send email for your domain.

Do I have it?

Confirm that DKIM DNS **records exist** for your domain, by using a DKIM validation tool (https://mxtoolbox.com/dkim.aspx, for example). Supply your domain name and "selector1" as a selector.

Here's an example of a correctly configured domain (Hosted on Office365):



Repeat the test for every domain from which you send email (*if you have more than one domain name*).

Confirm that DKIM **signing** is setup for your domain by following these Microsoft instructions:

1. Sign in to Office 365 with your work or school account.
2. Select the app launcher icon in the upper-left and choose Admin.
3. In the lower-left navigation, expand Admin and choose Exchange.
4. Go to Protection > dkim.
5. Select the domain for which you want to enable DKIM and then, for Sign messages for this domain with DKIM signatures, choose Enable. Repeat this step for each custom domain.

How do I get it?

Microsoft's guide is detailed (*but confusing*).

First, determine your **initial domain**. This domain was created for you when you setup Office365, and it ends in *.onmicrosoft.com*. Typically, your initial domain will be the your actual domain name (*i.e "widgets.com"*), with dots removed, followed by "*onmicrosoft.com*". So *widgets.com*'s **initial domain name** will be *widgetscom.onmicrosoft.com*.

Tip: You can also follow the steps above for enabling DKIM in Office365's Exchange Online admin. The resulting page will show you all your configured domains.

Secondly, determine your **domainGUID**. Unless you're a "GCC High" goverment customer, your **domainGUID** will simply be the same as your desired email domain - i.e, "*widgets.com*", with dots replaced with dashes. (*i.e.,* "*widgets-com*").

Now, that you have yoru **initial domain** and **domainGUID**, for every domain you want to protect, create 2 CNAME DNS records:

```
Host name:                      selector1._domainkey
Points to address or value:     selector1-<domainGUID>._domainkey.
<initialDomain>
TTL:                            3600

Host name:                      selector2._domainkey
Points to address or value:     selector2-<domainGUID>._domainkey.
<initialDomain>
TTL:                            3600
```

In the example of widgets.com, the following 2 records will be created:

```
Host name:                      selector1._domainkey
Points to address or value:     selector1-widgets.com._domainkey.widgets-
com.onmicrosoft.com
TTL:                            3600

Host name:                      selector2._domainkey
Points to address or value:     selector2-widgets.com._domainkey.widgets-
com.onmicrosoft.com
TTL:                            3600
```

Now enable DKIM **signing** for your domain by following these Microsoft instructions:

1. Sign in to Office 365 with your work or school account.
2. Select the app launcher icon in the upper-left and choose Admin.
3. In the lower-left navigation, expand Admin and choose Exchange.
4. Go to Protection > dkim.
5. Select the domain for which you want to enable DKIM and then, for Sign messages for this domain with DKIM signatures, choose Enable. Repeat this step for each custom domain.

(*Note : If the option to enable DKIM signing for your custom domain doesn't exist, you may need to use PowerShell*)

DMARC

What is it?

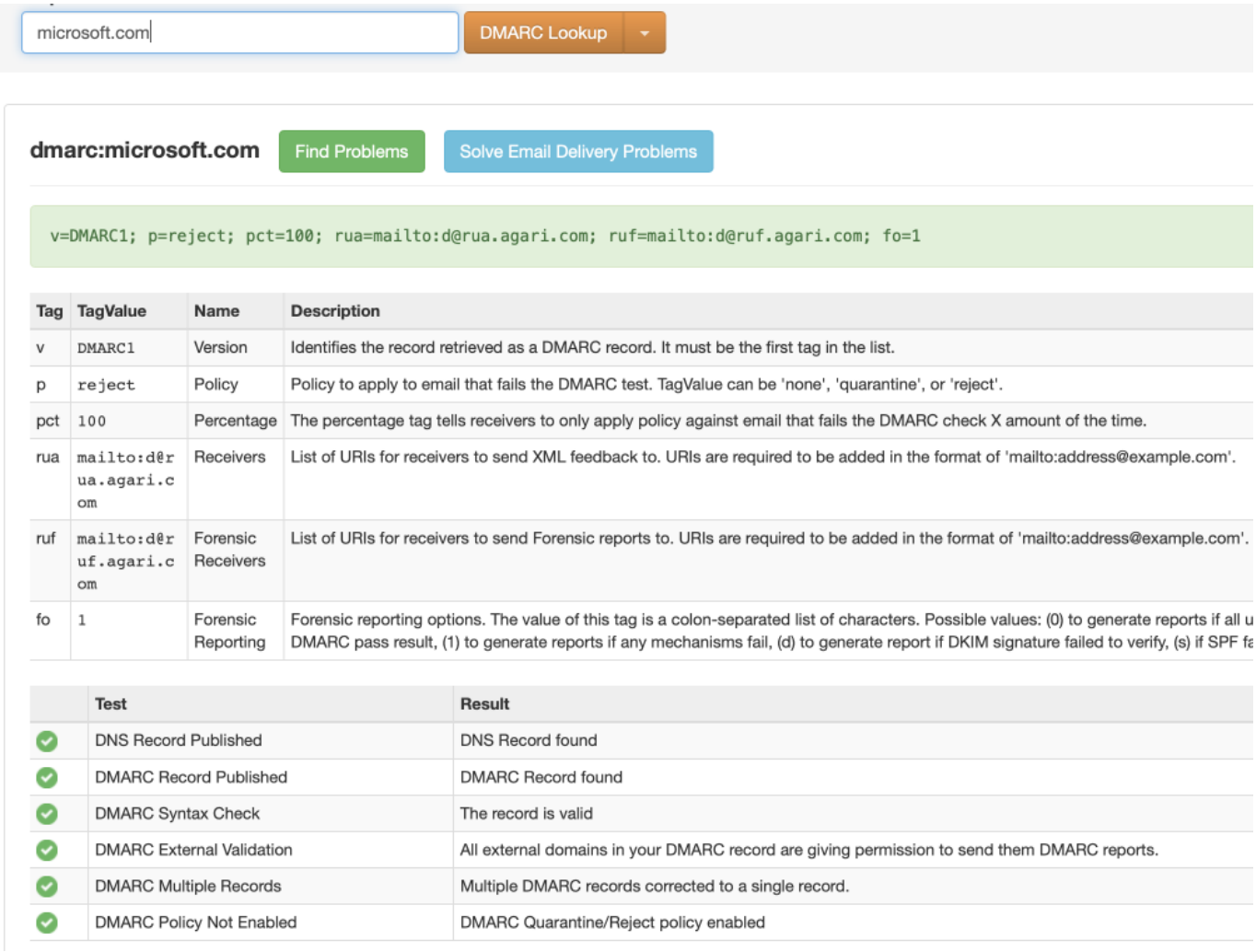
Domain-based Message Authentication, Reporting, and Conformance (DMARC) augments SPF, by testing not only the "envelope sender" of an email (***the address that bounces would go to***), but also the purported "From" address of the sender.

Unlike SPF, DMARC offers far more flexibility regarding what remote mail systems **do** with email which fails validation - you can choose to reject/quarantine a percentage of emails, have delivery reports sent to a nominated email address daily, etc.

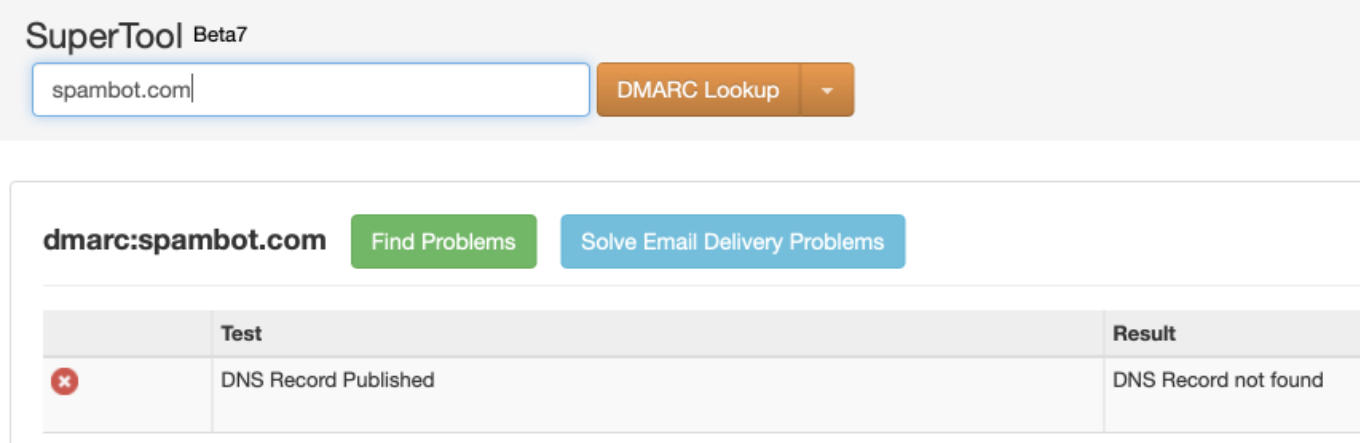
Do I have it?

Confirm that DMARC DNS TXT **records exist** for your domain, by using a DMARC validation tool (https://mxtoolbox.com/dmarc.aspx, for example). Supply your domain name and click `DMARC Lookup`.

Here's an example of a correctly configured domain:



And here's an example of an unconfigured domain:



How do I get it?

To protect your outgoing email with DMARC, setup a DNS TXT record.

Microsoft provides a guide, as does Google. You can also use an online DMARC record generator.

At the most basic (*and harmless*) level, add a TXT record like this to your domain:

```
_dmarc.yourdommain.com --> v=DMARC1; p=none;
rua=mailto:postmaster@yourdomain.com
```

If you want to be more aggressive, and instruct remote servers to **reject** any emails which appear to be spoofed from you, use a record like this:

```
_dmarc.yourdommain.com --> v=DMARC1; p=reject;
rua=mailto:postmaster@yourdomain.com
```

You can also stagger the rollout of DMARC, by instructing remote servers to reject only 10% of your email, and gradually increase this percentage:

```
_dmarc.yourdommain.com --> v=DMARC1; p=none;
rua=mailto:postmaster@yourdomain.com; pct=10
```