

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:

SuperTool Beta7

SPF Record Lookup

spf:amazon.com Find Problems Solve Email Delivery Problems

```
v=spf1 include:spf1.amazon.com include:spf2.amazon.com include:amazonses.com -all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	spf1.amazon.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf2.amazon.com	Pass	The specified domain is searched for an 'allow'.
+	include	amazonses.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

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"*):

spf:dell.com

```
v=spf1 include:_spf.dell.com include:spf-00154904.pphosted.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	_spf.dell.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf-00154904.pphosted.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

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

spf:dell.com

```
v=spf1 include:_spf.dell.com include:spf-00154904.pphosted.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	_spf.dell.com	Pass	The specified domain is searched for an 'allow'.
+	include	spf-00154904.pphosted.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your 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.



DKIM Record Lookup

Domain Name

Selector [?]

DKIM Lookup

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

dkim:microsoft.com:selector1
Find Problems
dkim

```
v=DKIM1; k=rsa; p=MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQCkHq3ztGIm1R8a1D+7oZiaG5mTutFdf0lpKHRBZCPFG4sugV1E5F5F6JpwbJDzZmyIlgYfTgUkmY0vbHsoYvW7rddLKVTh+vE1S25P9coIHrw759hXbpPDSQ9JNP8aN+Bfrg6YMEWn0GA+PL+ZpyvswcB0jz9M6yMvow0xCHv5QIDAQAB; n=1024,1435867504,1
```

Tag	TagValue	Name	Description
v	DKIM1	Version	The DKIM record version.
k	rsa	Key type	The type of the key used by tag (p).
p	MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQCkHq3ztGIm1R8a1D+7oZiaG5mTutFdf0lpKHRBZCPFG4sugV1E5F5F6JpwbJDzZmyIlgYfTgUkmY0vbHsoYvW7rddLKVTh+vE1S25P9coIHrw759hXbpPDSQ9JNP8aN+Bfrg6YMEWn0GA+PL+ZpyvswcB0jz9M6yMvow0xCHv5QIDAQAB	Public Key	Public-key data. The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.
n	1024,1435867504,1	Notes	Notes that might be of interest.

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DKIM Record Published	DKIM Record found
✓	DKIM Syntax Check	The record is valid
✓	DKIM Public Key Check	Public key is present

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 **widgetscm.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" government 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 your **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:

DMARC Lookup

dmarc:microsoft.com Find Problems Solve Email Delivery Problems

```
v=DMARC1; p=reject; pct=100; rua=mailto:d@rue.agari.com; ruf=mailto:d@ruf.agari.com; fo=1
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. TagValue can be 'none', 'quarantine', or 'reject'.
pct	100	Percentage	The percentage tag tells receivers to only apply policy against email that fails the DMARC check X amount of the time.
rua	mailto:d@rue.agari.com	Receivers	List of URIs for receivers to send XML feedback to. URIs are required to be added in the format of 'mailto:address@example.com'.
ruf	mailto:d@ruf.agari.com	Forensic Receivers	List of URIs for receivers to send Forensic reports to. URIs are required to be added in the format of 'mailto:address@example.com'.
fo	1	Forensic Reporting	Forensic reporting options. The value of this tag is a colon-separated list of characters. Possible values: (0) to generate reports if all u DMARC pass result, (1) to generate reports if any mechanisms fail, (d) to generate report if DKIM signature failed to verify, (s) if SPF fe

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

And here's an example of an unconfigured domain:

SuperTool Beta7

DMARC Lookup

dmarc:spambot.com Find Problems Solve Email Delivery Problems

	Test	Result
✗	DNS Record Published	DNS Record not found

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