Anti Spoof using SPF, DKIM and DMARC
Attendee Handout
Not all cloud services are equal

External data sharing services include a variety of options.

External data sharing services are not all created equal. Some offer basic file sharing, while others provide advanced collaboration features. It's important to choose the right service for your needs.

For example, Google Drive offers basic file sharing, while Microsoft OneDrive provides additional collaboration features.

It's also important to consider the security and privacy of the service. Some services offer stronger encryption and privacy features than others.

Ultimately, the best service for you will depend on your specific needs and requirements.
aOS Conference KL
Azure, Office365 & SharePoint
23/10/2018

18 Sessions
14 International Speakers
11 MVPs
Who does Email Spoofing Affect?
Prevent Others from being cheated

Prevent Users from being cheated
Can attack both internal staff and external public
Online Stores are very vulnerable. Hackers target your customers, not you! (using your email)

admin@contosoOnline.com
Please Reset your Password !!!
What if there is a way to check the authenticity of an email? There is, via embedding SPF, DKIM and DMARC fields in the domain DNS.
How Office365 handles Spoof Prevention
Due to the Smart Phone, the IT user is actually quite IT Savvy outside of work.
Corporate IT tools usually lag behind compared to private smart phone tools.
As a result, users bring their free apps into the workplace, without IT approval or knowledge.
Office365 gives these users similar functionality, but offers world class protection.

<table>
<thead>
<tr>
<th>MS Office</th>
<th>Power BI</th>
<th>PowerApps</th>
<th>Flow</th>
<th>Delve</th>
<th>Staff Hub</th>
<th>Business Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange</td>
<td>SharePoint</td>
<td>Skype</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“Email”</td>
<td>“CMS, File Management”</td>
<td>“Communications”</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Management</td>
<td>Information Protection</td>
<td>Search &amp; Investigate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDM, EMS</td>
<td>AIP, DLP</td>
<td>Hold, eDiscovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azure AD – Free, Basic</td>
<td>Azure AD – P1 &amp; P2</td>
<td>Threat Mgmt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ATP, Adv Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On Premise Active Directory
Office365 Anti-Spoof for OutBound Messages
SPF is set when you first install Office365

<table>
<thead>
<tr>
<th>If you're using...</th>
<th>Common for Office 365 customers?</th>
<th>Add this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Any email system (required)</td>
<td>Common. All SPF TXT records start with this value</td>
<td>v=spf1</td>
</tr>
<tr>
<td>2. Exchange Online</td>
<td>Common</td>
<td>include:spf.protection.outlook.com</td>
</tr>
<tr>
<td>3. Exchange Online dedicated only</td>
<td>Not common</td>
<td>ip4:23.193.224.0/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip4:205.101.224.0/19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip4:40.103.0.0/16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>include:spf.protection.outlook.com</td>
</tr>
<tr>
<td>4. Office 365 Germany, Microsoft Cloud Germany only</td>
<td>Not common</td>
<td>include:spf.protection.outlook.de</td>
</tr>
<tr>
<td>5. Third-party email system</td>
<td>Not common</td>
<td>Include:&lt;domain name&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Where domain name is the domain name of the third party email system.</td>
</tr>
<tr>
<td>6. On-premises mail system. For example, Exchange Online Protection plus another mail system</td>
<td>Not common</td>
<td>Use one of these for each additional mail system:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ip4:&lt;IP address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- ip6:&lt;IP address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- include:&lt;domain name&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Where the value for &lt;IP address&gt; is the IP address of the other mail system and &lt;domain name&gt; is the domain name of the other mail system that sends mail on behalf of your domain.</td>
</tr>
<tr>
<td>7. Any email system (required)</td>
<td>Common. All SPF TXT records end with this value</td>
<td>&lt;enforcement rule&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This can be one of several values. We recommend that you use -all.</td>
</tr>
</tbody>
</table>

v=spf1 include:spf.protection.outlook.com -all
Sender Rewrite Scheme (SRS) - 15 Jul 18

• Takes care of SPF issues when
  • Auto-forwarded Message using SMTP Fwd, Mailbox/Transport Rule Redirect
  • Auto-forward from On-Prem Exchange through O365

P1 From: bob@fabrikam.com
  From: bob@fabrikam.com

John.work@contoso.com

John.home@example.com

P1 From: john.work+SRS=44ldt=1X=fabrikam.com=bob@contoso.com
  From: bob@fabrikam.com
O365 automatically enables DKIM if not set

If we have not enabled DKIM, Office 365 automatically creates a 1024-bit DKIM public key for all the custom domains and the associated private key which are stored internally in Microsoft datacenters. By default, Office 365 uses a default signing configuration for all domains that do not have a policy in place. This means that if DKIM is not manually setup, Office 365 will use its default policy and keys to enable DKIM. Also, if we disable DKIM signing after enabling it, Office 365 will automatically apply the Office 365 default policy for this domain.

---

**Enabled – uses headers in DNS**

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
   d=vincentchoy.com; s=selector1;
   h=From:Date:Subject:Message-Id:Content-Type:MIME-Version;
   b=qj1WAoF5f1HqjGr4y3V7Pp4+yR2GyXu74Z9dAaOnZG7mDjzG3Pvfr7+ZqXJu1QcVxY1ctSdP6Jt20yZv
Sc9eXoYUfryBxZs4cGCBbB6Nk+aU4H3+2S502wSnG7N/t+3Wzv1O5E2OpdznVb/3i+0m7OaJi8bA/5H1Cq
EBl23hPXO2xHxQ8q6wmw5ZQ==
```

**Disabled – Microsoft auto-turns on dkim**

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
   d=fedelissb.onmicrosoft.com; s=selector1-fedelis-com-my;
   h=From:Date:Subject:Message-Id:Content-Type:MIME-Version;
   b=n7i3VqSk29s1o5J1G9+Osa7QyPK5E8tOQ4kFjO/THDekrrkKz7s4qfBq4z4n+aj+L1w3vL3xNvG1R3x
w8zsdA1j7E1g98H9/OlYBMv16jY64OZ5ZJw7+bsEYbr0IQdTVX4EVPON8kL8bFMTuH7n7/gP+6i8CqN3
xj+Pj60e8PHQOeYTl9TfV2b9o0y+Z2s2eLcycx2Tb49RTStVbbk4N9rE==
```
MS-Default DKIM verification algorithm

1. IF you see d=*.onmicrosoft.com, **AND**
2. IF you remove 'selector1/2-', **AND**
3. IF you replace any dots in the From: address with dashes (e.g., fabrikam.com -> fabrikam-com) [1] and it matches the unremoved parts in the selector (e.g., selector1-fabrikam-com)
4. THEN you can consider the message implicitly DMARC aligned.

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=fedelissb.onmicrosoft.com; s=selector1-fedelis-com-my;
h=From:Date:Subject:Message-ID:Content-Type:MIME-Version
Microsoft will tell you what to put in DNS

CNAME record does not exist for this config. Please publish the following two CNAME records first.

selector1-Fedelis-sg._domainkey.fedelissb.onmicrosoft.com
selector2-Fedelis-sg._domainkey.fedelissb.onmicrosoft.com

Fedelis.sg

Sign messages for this domain with DKIM signatures: Disabled

Enable

Status:
Not signing DKIM signatures for this domain.

Last checked on:
28/1/2016 10:33 AM
DMARC will fail if use O365 “auto” DKIM

Step 3: Set up DKIM for your custom domain in Office 365

Once you have set up SPF, you need to set up DKIM. DKIM lets you add a digital signature to email messages in the message header. If you do not set up DKIM and instead allow Office 365 to use the default DKIM configuration for your domain, DMARC may fail. This is because the default DKIM configuration uses your initial onmicrosoft.com domain as the 5322.From address, not your custom domain. This forces a mismatch between the 5321.MailFrom and the 5322.MailFrom addresses in all email sent from your domain.
DKIM will fail if there is a mail relay

Remember that if you have another mail server positioned after Office 365 that relays out to the Internet, it may modify the message content and cause the DKIM signature not to verify. If this occurs, you should ensure that Office 365 is the last service to relay out to the Internet, otherwise you may get some email bounces due to a broken DKIM signature.
DMARC tells the recipient email servers what to do when receiving mails from you -

• What to do if a mail is suspicious – Pass, Quarantine or Reject
• Where to apply this policy – Main Domains / Sub Domains
• How many emails to examine?
• How often to send reports?
• Where to send the reports?

* Note – It is up to the recipient email servers to execute these checks. Some old or basic email receivers may not perform any or all of these instructions. However you have done your part by doing these settings in your DNS.
In this example, the sender requests that the receiver outright reject all non-aligned messages and send a report, in a specified aggregate format, about the rejections to a specified address. If the sender was testing its configuration, it could replace “reject” with “quarantine” which would tell the receiver they shouldn’t necessarily reject the message, but consider quarantining it.

DMARC records follow the extensible “tag-value” syntax for DNS-based key records defined in DKIM. The following chart illustrates some of the available tags:

<table>
<thead>
<tr>
<th>Tag Name</th>
<th>Purpose</th>
<th>Sample</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>Protocol version</td>
<td>v=DMARC1</td>
</tr>
<tr>
<td>pct</td>
<td>Percentage of messages subjected to filtering</td>
<td>pct=20</td>
</tr>
<tr>
<td>ruf</td>
<td>Reporting URI for forensic reports</td>
<td>ruf=<a href="mailto:authfail@example.com">mailto:authfail@example.com</a></td>
</tr>
<tr>
<td>rua</td>
<td>Reporting URI of aggregate reports</td>
<td>rua=<a href="mailto:agrep@example.com">mailto:agrep@example.com</a></td>
</tr>
<tr>
<td>p</td>
<td>Policy for organizational domain</td>
<td>p=quarantine</td>
</tr>
<tr>
<td>sp</td>
<td>Policy for subdomains of the OD</td>
<td>sp=reject</td>
</tr>
<tr>
<td>adkim</td>
<td>Alignment mode for DKIM</td>
<td>adkim=s</td>
</tr>
<tr>
<td>aspf</td>
<td>Alignment mode for SPF</td>
<td>aspf=r</td>
</tr>
</tbody>
</table>

Eg Microsoft’s DMARC

_dmarc.microsoft.com. 3600 IN TXT "v=DMARC1; p=none; pct=100; rua=mailto:d@rua.agari.com; ruf=mailto:d@d@ruf.agari.com; fo=1"
DMARC - Timid

_dmarc  TXT ( "v=DMARC1;p=none;sp=reject;pct=10;"
           "adkim=r;aspf=r;fo=1;ri=86400; rua=mailto:dmarc-admin@example.net")

P=none    - No advice for main domain
SP=reject - Reject spoof for Sub-Domain
Pct = 10   - Applies to 10% of mail
Adkim=r    - relaxed : allow subdomains for dkim check (s = strict)
Aspf =r    - relaxed : allow subdomains for spf check (s = strict)
Ri=86400   - daily report (secs)
Rua        - aggregated mail reports to ....
DMARC Aggresive

_dmarc TXT ( "v=DMARC1;p=reject;sp=reject;pct=100;"
"aspf=r;fo=0;ri=86400;rua=mailto:dmarc-admin@example.net")

P=reject - Reject spoof for main domain
SP=reject - Reject spoof for Sub-Domain
Pct = 10 - Applies to 100% of mail
Adkim=r - relaxed: allow subdomains for dkim check
Aspf =r - relaxed: allow subdomains for spf check
Ri=86400 - daily report (secs)
Rua - aggregated mail reports to ....
DMARC Reporting

- Knowing if your anti-spoof settings are working is important
- Knowing if scammers are using your email domains to spoof others is important
- Allows you to take proactive countermeasures against spoofing
- Allows you to protect your company reputation
- Allows you to protect your own company users
- Allows you to protect your customers and suppliers
DMARC generates 2 kinds of reports

• Aggregate reports - reports provide information about which emails are authenticating against SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC, and which are not.

• Forensic reports - In addition to providing information about which emails are authenticating against SPF, DKIM, and DMARC (as aggregate reports do) forensic reports include additional information such as the subject line and header information as well as, most importantly any URLs (URIs) included in the message.

• Need analysis tools to interpret DMARC Reports
Authentication-Results: spf=softfail (sender IP is 46.167.245.205)
smtp.mailfrom=vincentchoy.com; fedelis.com.my; dkim=none (message not signed)
header.d=None;fedelis.com.my; dmarc=fail action=None
header.from=vincentchoy.com;compauth=fail reason=001
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning
Aggregate report example

Emails will be sent to mailbox based on DMARC settings.
Forensic report example
Having a reporting tool to analyze the results is critical
Reporting Tool can show if all your sending servers are defined

Audit of known commercial entities (legitimate) using the <Customer> domain.

<table>
<thead>
<tr>
<th>Source</th>
<th>Volume</th>
<th>SPF</th>
<th>DKIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF-Identified Servers</td>
<td>5,994,568</td>
<td>99.8%</td>
<td></td>
</tr>
<tr>
<td>MailChimp</td>
<td>756,170</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Related Servers</td>
<td>632,820</td>
<td>59%</td>
<td></td>
</tr>
<tr>
<td>SendGrid, Inc.</td>
<td>13,758</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Google, Inc.</td>
<td>1,913</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Salesforce.com</td>
<td>11</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>NetSuite Inc.</td>
<td>8</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>ExactTarget (now Salesforce)</td>
<td>3</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>
Reporting tool can show if your domains are listed as suspicious

Legitimate domains incorrectly configured may be targeted by anti-spam servers.

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Frmr. domain count</th>
<th>Message count</th>
<th>IP count</th>
<th>Alignment</th>
<th>SPF; DKIM; DkimSig; DkimDomain</th>
<th>DMARC Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>*nxdomain</td>
<td>1</td>
<td>3</td>
<td>14058</td>
<td>21</td>
<td>0; 0; 0</td>
<td>*/.nxdomain</td>
</tr>
<tr>
<td>*.msa.com</td>
<td>1</td>
<td>2154</td>
<td>1</td>
<td>1</td>
<td>0; 0; 0</td>
<td>*/.msa.com</td>
</tr>
<tr>
<td>*.topdomain.com</td>
<td>1</td>
<td>1518</td>
<td>1</td>
<td>2</td>
<td>0; 0; 0</td>
<td>*/.topdomain.com</td>
</tr>
<tr>
<td>*.nl-reverse.com</td>
<td>1</td>
<td>1775</td>
<td>2</td>
<td>0</td>
<td>0; 0; 0</td>
<td>*/.nl-reverse.com</td>
</tr>
<tr>
<td>*webhostinghub.com</td>
<td>1</td>
<td>1121</td>
<td>1</td>
<td>1</td>
<td>0; 0; 0</td>
<td>*/.webhostinghub.com</td>
</tr>
<tr>
<td>*.urljet.com</td>
<td>1</td>
<td>737</td>
<td>1</td>
<td>1</td>
<td>0; 0; 0</td>
<td>*/.urljet.com</td>
</tr>
<tr>
<td>*.demonet-phil.com</td>
<td>1</td>
<td>329</td>
<td>2</td>
<td>0</td>
<td>0; 0; 0</td>
<td>*/.demonet-phil.com</td>
</tr>
<tr>
<td>*.domains.ph</td>
<td>2</td>
<td>270</td>
<td>1</td>
<td>1</td>
<td>0; 0; 0</td>
<td>*/.domains.ph</td>
</tr>
<tr>
<td>*.soapcloud.co.uk</td>
<td>2</td>
<td>243</td>
<td>1</td>
<td>1</td>
<td>0; 0; 0</td>
<td>*/.soapcloud.co.uk</td>
</tr>
<tr>
<td>*.smart.com.ph</td>
<td>1</td>
<td>216</td>
<td>3</td>
<td>0</td>
<td>0; 0; 0</td>
<td>*/.smart.com.ph</td>
</tr>
<tr>
<td>*websitewelcome.com</td>
<td>1</td>
<td>213</td>
<td>132</td>
<td>0</td>
<td>0; 0; 0</td>
<td>*/.websitewelcome.com</td>
</tr>
<tr>
<td>*.me.com</td>
<td>1</td>
<td>208</td>
<td>1</td>
<td>1</td>
<td>0; 0; 0</td>
<td>*/.me.com</td>
</tr>
<tr>
<td>*.web.com.ph</td>
<td>3</td>
<td>182</td>
<td>8</td>
<td>0</td>
<td>0; 0; 0</td>
<td>*/.web.com.ph</td>
</tr>
<tr>
<td>*.punt.net</td>
<td>1</td>
<td>173</td>
<td>3</td>
<td>0</td>
<td>0; 0; 0</td>
<td>*/.punt.net</td>
</tr>
<tr>
<td>*.bcd40domain.com</td>
<td>2</td>
<td>133</td>
<td>1</td>
<td>1</td>
<td>0; 0; 0</td>
<td>*/.bcd40domain.com</td>
</tr>
<tr>
<td>*.onestopwebworlds.com</td>
<td>1</td>
<td>133</td>
<td>1</td>
<td>0</td>
<td>0; 0; 0</td>
<td>*/.onestopwebworlds.com</td>
</tr>
</tbody>
</table>
Reporting tool will generate Forensic Report Summary - this can show what is the Lure used to trick users – allow you to take counter measures

DMARC failure based on forwarded email – SPF and DKIM failure
Fedelis works with dmarcian reporting tool and advisory services to help you secure your domain against spoof
Office365 Anti-Spoof for InBound Messages
Office365 and Incoming Messages

- Uses sender SPF, DKIM and DMARC settings to evaluate spoof
Fedelis.com.my

Bill Gates

I will pay you USD 1 Million. Click the link now.

SPF
DKIM
DNS
DMARC

Vincent Choy
This wasn’t sent from vc@Fedelis.com.my

SPF Fail – did not come from O365, came from emkei.cz instead
Office365 and Incoming Messages

• Who is the sending domain / sending IP?
• How often does the sender or recipient exchange email?
Lee Kuan Yew

To vc

Retention Policy Junk Email (30 days)

Links and other functionality have been disabled in this message. To turn this message was marked as spam using a junk filter other than the Out!

Call me now
This wasn’t sent from me@vincentchoy.com

“This” in front of “all” means that any servers not listed in this SPF record should be treated as a "softfail", which means that mail can be allowed through but should be tagged as spam or suspicious.
## Legitimate Internal Spoof Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd party senders who use your domain to send bulk mail to your own employees for company polls</td>
<td></td>
</tr>
<tr>
<td>External company/vendor that creates and sends out advertising or product updates on your organization’s behalf</td>
<td></td>
</tr>
<tr>
<td>An assistant who regularly needs to send email for another person within your organization</td>
<td></td>
</tr>
<tr>
<td>An application that is configured to spoof its own organization in order to send internal notifications by email</td>
<td></td>
</tr>
</tbody>
</table>

## Legitimate External Spoof Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An external company sends email on behalf of another company (for example, an automated report, or a software-as-a-service company).</td>
<td></td>
</tr>
<tr>
<td>The sender is on a discussion mailing list, and the mailing list is relaying the email from the original sender to all the participants on the mailing list.</td>
<td></td>
</tr>
</tbody>
</table>
Reducing Genuine Spoof marked as spam

• Correctly configuring SPF and DKIM to include 3rd Party Services

• White List Sender IP Address in Exchange Admin Center / ATP

• Add Exchange Transport Rule to bypass filtering for specific address
Office 365 Advanced Threat Protection

Protect your email, files, and Office 365 applications against unknown and sophisticated attacks.

Customers with subscriptions to select Exchange or Office 365 plans can add Advanced Threat Protection for RM8.40 per user.

Find out how

Price does not include tax.
Advanced Threat Protection (ATP)

Office365 Standard Plans

Office365 with ATP
## Edit your policy Fedelis Anti-Phishing Policy

### Customize the Impersonation, Spoofing, and Advanced settings for this policy.

<table>
<thead>
<tr>
<th>Priority</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>On</td>
</tr>
<tr>
<td>Last modified</td>
<td>26 June 2018</td>
</tr>
</tbody>
</table>

### Policy settings

- **Policy name**: Fedelis Anti-Phishing Policy
- **Brief description**: Custom settings of AP Policy
- **Applied to**: If the recipient domain is fedelis.com.my

#### Impersonation

- **Users to protect**: Off
- **Protect all domains I own**: Off
- **Protect specific domains**: Off
- **Action > User impersonation**: Don't apply any action
- **Action > Domain impersonation**: Don't apply any action
- **Safety tips > User impersonation**: Off
- **Safety tips > Domain impersonation**: Off
- **Safety tips > Unusual characters**: Off
- **Mailbox Intelligence**: On

#### Spoof

- **Enable antispooﬁng protection**: On
- **Move message to the recipients' Junk Email folders**: Move message to the recipients' Junk Email folders

### Advanced settings

- **Advanced phishing thresholds**: 1 - Standard
Advanced Threat Protection (ATP)

Office365 Standard Plans

Anti-spam settings

Our standard settings cover the basics so you can have peace of mind that your organization is protected from spam. But if you want more control, switch to custom settings and take advantage of a robust set of features, including custom spam filter policies that you can apply to users and groups. Learn more about anti-spam settings.

Custom settings

Custom settings

Office365 with ATP

Custom settings

Custom settings

Review senders that are spoofing your domain. You can block or allow these senders from spoofing your domain. Learn about spoof indicator.
Review senders that are spoofing your domain. You can block or allow these senders from spoofing your domain. Learn about spoof intelligence

Show me senders I already reviewed
Review new senders

---

## Decide if these senders are allowed to spoof your users

These senders might be spoofing users in your organization. Learn about spoof intelligence

### What we already did

We blocked senders who were exhibiting malicious behavior and allowed those who appear legitimate.

### What you need to do

Review the list and decide if the sender is allowed to spoof users. Some senders might be spoofing more than one user. If that's the case, you can either allow them to spoof all users or use the Detailed view to make a decision for each spoofed user.

<table>
<thead>
<tr>
<th>Spoofed User</th>
<th>Sending Infrastructure</th>
<th># of messages</th>
<th># of user complaints</th>
<th>Authentication result</th>
<th>Decision set by</th>
<th>Last seen</th>
<th>Allowed to spoof</th>
</tr>
</thead>
<tbody>
<tr>
<td>unsecure.com</td>
<td>103.18.3.24</td>
<td>1</td>
<td>0</td>
<td>Failed</td>
<td>7/6/2018</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ben@secure</td>
<td>103.32.112.0/24</td>
<td>1</td>
<td>0</td>
<td>Failed</td>
<td>8/5/2018</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>skin.com</td>
<td>104.47.104.0/24</td>
<td>1</td>
<td>0</td>
<td>Failed</td>
<td>7/6/2018</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>muscle.com</td>
<td>104.47.136.0/24</td>
<td>1</td>
<td>0</td>
<td>Failed</td>
<td>4/6/2018</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><a href="mailto:someone@faked.com">someone@faked.com</a></td>
<td>104.47.31.0/24</td>
<td>1</td>
<td>0</td>
<td>Failed</td>
<td>5/6/2018</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Questions?
Contact vc@Fedelis.com.my