Setting Up DMARC

Setting up DMARC (Domain-based Message Authentication, Reporting, and Conformance) can help improve email security and prevent domain spoofing. DMARC can be configured with different levels of strictness, including relaxed (p=none) and strict (p=quarantine or p=reject) policies. Here's a tutorial on how to set up both relaxed and strict DMARC policies:

Setting Up Relaxed DMARC (p=none)

Relaxed DMARC allows you to monitor email traffic without taking immediate action on failed messages. This is a good starting point to gain insights into your email authentication status.

1. **Access Your DNS Records**: DMARC records are published in your domain's DNS records. Log in to your domain registrar or DNS hosting provider's dashboard.
2. **Create a DMARC Record**: Add a DMARC TXT record to your domain's DNS. The record should have a `p=none` policy to indicate that you're not taking immediate action on failed messages. Here's an example:

   ```
   v=DMARC1; p=none; rua=mailto:dmarc@example.com;
   ```

   - `v=DMARC1`: This indicates that it's a DMARC record.
   - `p=none`: Specifies that no action should be taken on failed messages.
   - `rua=mailto:dmarc@example.com`: This is the email address where DMARC aggregate reports will be sent.
3. **Publish the Record**: Save the DNS record. It might take some time for DNS changes to propagate across the internet.
4. **Monitor Reports**: As DMARC reports start coming in, review them to gain insights into email sources and authentication status. Make adjustments to your email infrastructure as needed to improve authentication.

Setting Up Strict DMARC (p=quarantine or p=reject)

Strict DMARC policies are more secure but can potentially impact legitimate email delivery. Use strict policies when you're confident in your email authentication setup.

1. **Access Your DNS Records**: Access your domain's DNS records as described in the previous section.
2. **Create a DMARC Record**: Add a DMARC TXT record to your domain's DNS. Set the policy to `p=quarantine` or `p=reject` to specify stricter actions for failed messages:
   - `p=quarantine`: Suspicious emails will be delivered to the recipient's spam or quarantine folder.
   - `p=reject`: Fails suspicious emails entirely.

Example for `p=quarantine`:

```
v=DMARC1; p=quarantine; rua=mailto:dmarc@example.com;
```

3. **Publish the Record**: Save and publish the DMARC record in your DNS settings.
4. **Gradual Implementation**: When moving to strict DMARC policies, consider implementing it gradually. Start with `p=none` or `p=quarantine`, monitor reports, and gradually move to `p=reject` as you become confident in your email authentication setup.
5. **Monitor and Adjust**: Continuously monitor DMARC reports and adjust your email infrastructure to ensure legitimate emails aren't affected while blocking suspicious ones.

Remember that strict DMARC policies can affect email delivery, so be cautious when implementing them. Regularly review DMARC reports and refine your DMARC policy based on your organization's needs and email authentication progress.

Revision #3
Created 7 October 2023 10:51:35 by Cindy
Updated 7 October 2023 15:33:20 by Cindy