Best Practices for Email Senders

Don Owens, Senior Architect
Talos Group, Cisco Systems
April 2017

Who is Talos?

Talos

- Data for Email and Web Security Appliances (IronPort ESAs and WSAs), etc.
- Data for Cloud Email and Web Security
- 19.7 billion total threat blocks daily (i.e., 2.7 threat blocks for every person in the world)
- 16 billion web requests daily
- 500 billion emails

Best Practices

Don't look like the bad guys.

Don't look like the bad guys

- No DGAs
  - Don't generate hosts/subdomains using an algorithm
  - n3456x35.example.com looks evil – don't do it
- Anchor text
  - if the anchor text for a link is a URL, it should match the destination (URL in the href field)

Tell us who you are.

TALOS

Show us you're not a robot

- Use a real public host name for HELO
  - localhost.localdomain ← don't do this 🙈
  - mta1.example.com ← do this 😎
- HELO and PTR match
  - Configure your MTA to HELO with the same host name string as the PTR record for your IP address.

TALOS

Authentication

- SPF
  - Easy setup in DNS
- DKIM
  - Easy to set up in DNS, but also requires configuration in your MTA
- DMARC
  - Based on SPF and DKIM
  - Allows you to specify what the receiver should do if DMARC checks fail
  - Allows you to specify reporting addresses for DMARC failures

Show us that you're a professional.

Show us that you're a professional

- Marketing: include unsubscribe links and headers
- A mail server should do one thing. Only send and/or receive mail. Don't run DNS, web servers, etc., on the same IP
- Don't use domain privacy services

Warm up your IPs and domains

Talos

Require double opt-in

- It's very important to get permission to send marketing to a recipient.
- Not doing so may or may not increase your revenue in the short term, but it cost everyone money in the end, and it damages your reputation.

Monitor bounces

If too many of your emails are bounced (due to invalid recipients), it will look like you're performing a directory harvest attack.

Don't use generic friendly-froms

Always include your brand name in the From: header.

- Bad:
  - Updates
  - Account Verification
  - Customer Service

- Good:
  - Acme Updates
  - Acme Account Verification
  - Acme Customer Service

TALOS

URL shortners and redirectors

There's a debate around this one, as some mail security providers feel this is needed to some extent, to protect customers with click-time protection.

The issue is that it's reputation hijacking.

If you use a URL shortener/redirector, it’s best to make sure it’s on your own domain (same as sender).

List washing

One of the fastest ways to destroy trust, and therefore your reputation.

- Don’t do it!
- Don’t do it!
- Just don’t!

Don't buy or rent lists

- If you're buying a list, the recipients on that list didn't opt-in.
- Someone on those lists will eventually report your messages as spam. This will take time to recover from.

It's all about building trust

TaLOS

Future of Reputation

What's Next?

- Sender domain block list from SpamCop, similar to the SpamCop IP blocklist
- SBRS Domains – sender domain reputation for Cisco customers

talosintelligence.com
blog.talosintel.com
@talossecurity