EASYDMARC

DMARC for Non-Profit Industry:

risks and solutions

Table of Contents

Why Non-Profit Industry is an attractive target of cyberattacks ?

The NonProfit Times study shows the total revenue of the largest NPOs has increased to 84.7 billion dollars that derives at least 10 percent revenue from public support.
The increase was the result of skyrockets across every revenue category.

Public support increased by 3.43% totaling $46.637 billion, which amounts to the 55% of annual income. Revenues for program services grew 11.5%, to $21.4 billion. Management costs increased 7% to $6.27 billion, while fundraising costs reached to $3.965 billion or by 5.13%. Finally, program expenses were up almost 4%, making it to $69.5 billion in total.

NPOs provide the most important services with a dedicated team of voluntary workers and donors.
Due to NPOs' fewer IT staff and limited resources, cybercriminals consider NPOs as easy prey to a wealth of personal data concerning their staff, donors and volunteers, and the communities they serve.
A number of NPOs have fallen victim to cybercrime which resulted in a loss of income.

Risks associated with cyberattacks

Because of the absence of cybersecurity strategies and policies in place - NPO systems can be compromised in an instant.

The risks are, but are not limited to:

Loss of donation.

Cost of recovering the funds lost.

Donor database data compromise.

1 https://www.thenonprofittimes.com/report/nonprofits-have-struggled-to-meet-service-organizational-demands/

EASYDMARC
www.easydmarc.com
+1-888-563-5277
sales@easydmarc.us

Cyberattacks NPOs are facing and what it can lead to:

Spear phishing is the main source of cybercrime in the NPO industry.
E-mails are designed to appear legitimate, look like the recipient knows, and trusts like senior management or a valued donor. Once the crime has been committed nothing can be done to recover lost funds. Specifically, the systems NPOs have access to and the data they store make attractive targets to cybercriminals. The dependencies on payment portals, donor CRM systems, and storing customer SSN or Corporate Tax IDs are consistent with the IT infrastructure of banks and financial institutions. So not only is the NPO a target for hackers, the systems the NPO integrates with, and their member community are sought-after targets for cybercriminals.

DMARC coverage for the NPO industry

The best option for NPOs to prevent cyberattacks will be the adoption of DMARC. With the help of DMARC security, NPOs will be able to safeguard their domain from being spoofed and can block unauthorized email and make email safer by significantly improving the efficiency of their email security.
You can rely on DMARC for valuable data about cyberattacks like phishing and spoofing against your company and it will empower NPOs to better help the people whose health and education depend on their hard work.

By adopting DMARC standard, NPOs can:

- Secure, detect and protect email spoofing of their domains
- Reject emails sent by unauthorized senders
- Stop display-name and lookalike domains spoofing
- Monitor risky domains registered by fraudsters

Benefits of DMARC

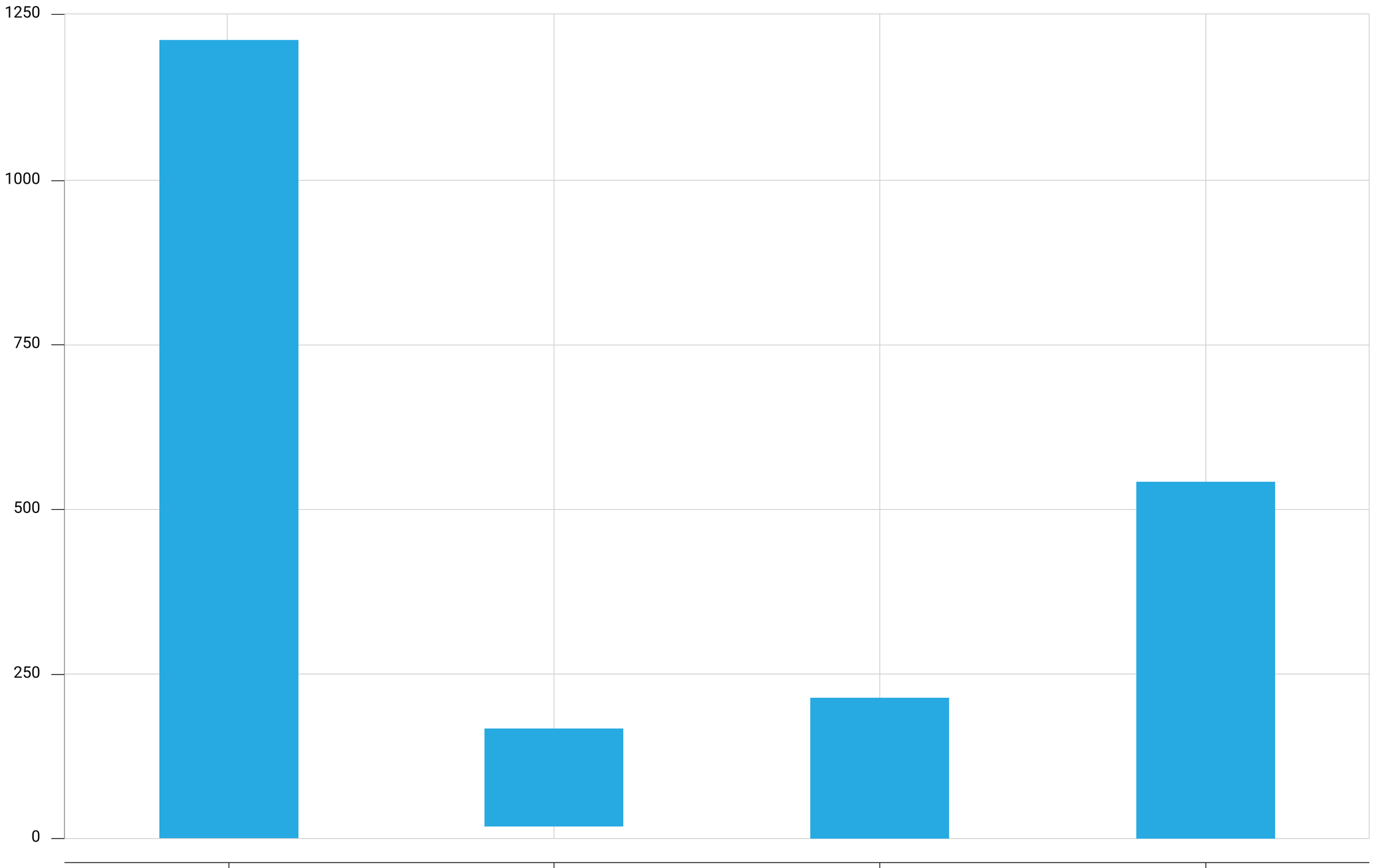
- Increased email deliverability
- Brand protection
- Security and visibility
- Delivery and communication
- Reputation and revenue

Do Non-Profits Lag in DMARC Adoption ?

After analyzing the top 2000 domains in the non-profit sector, we found that the majority of NPOs lacked DMARC policies designed to block the unauthorized use of their email domains, also known as “phishing”. On a more promising note, the percentage of NPOs with domains protected by DMARC has increased by 43% since December of 2020. Unfortunately, this translates to 57% of NPOs that remain vulnerable to phishing attacks that could directly target their donors, volunteers, and even their own staff. EasyDMARC has done research on NPOs to find out if they are far behind in DMARC adoption even though they continue to hold a significant amount of personal data. Therefore DMARC is a must for every domain owner in NPOs to protect and empower their organization.

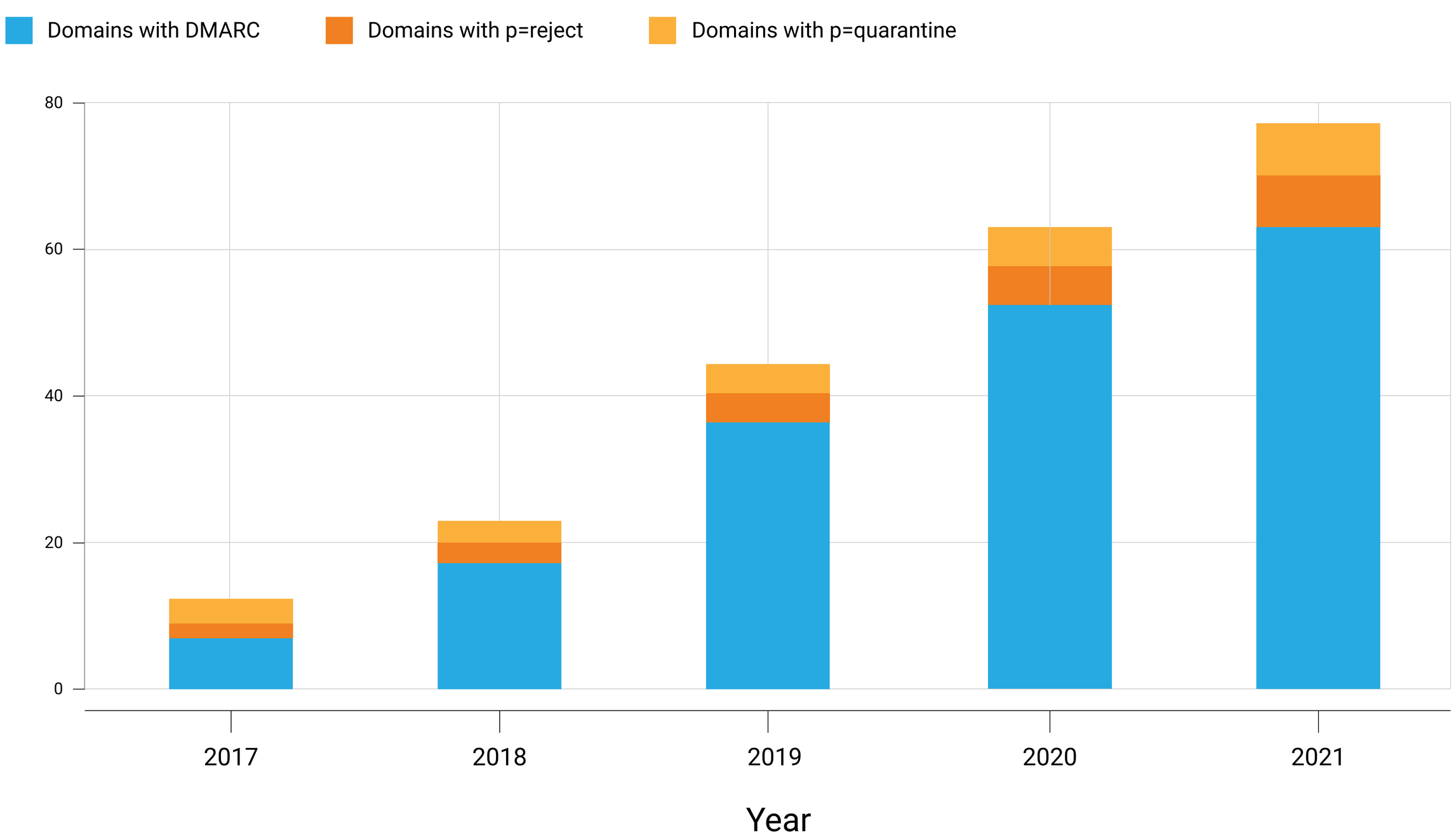
Last year, the number of DMARC domains worldwide increased by approximately 300 % to just under 2 million. The following graph shows the number of NPO domains that published DMARC policies. The number of domains that publish a "p=none" policy is continually increasing with a corresponding decrease in the “p=quarantine” and “p=reject” policies.

NPO Industry DMARC policies



DMARC Report Card for Non-Profit Organizations

According to our analysis, the number of valid DMARC policies present in DNS of NPOs increased by 23% over 2020.
Based on our research, approximately 40% of mentioned top 2000 nonprofits are DMARC users, which means that the rest of the nonprofits need DMARC adoption and implementation to keep their customers and employees safe from phishing attacks.
The graph below shows the policies during the last 5 years and an increase in overall DMARC adoption from 2017 to 2021. There is a gradual increase in the number of domains with DMARC set to “p=reject” or “p=quarantine” policies.



Even on a global scale, DMARC adoption for NPOs isn’t as high.

In Canada, **95%** of non-profit organizations, followed by Australia (**92%**) and the US(91%), have not implemented a DMARC policy at all. It means that less than 1% of NPOs had a DMARC policy set to reject — the highest level of brand protection.