Industry Report

Email Authentication Adoption in the UK Charitable Sector

Fewer than 1% of UK charitable organisations are protected against online fraud via email impersonation

February 2017

Fewer than 1% of UK charitable organisations are protected against online fraud via email impersonation

Summary

OnDMARC analysed more than 78,000 domains from the UK charity sector to understand how many of the charities implement email authentication protocols to protect their organisations, their users and their donors from cyber-attacks.

The study looked specifically at the adoption of the DMARC protocol which is the main standard for email authentication. The protocol has been endorsed by the UK government and required to all government agencies in the UK.

The study found that fewer than 1% of those organisations have implemented DMARC and of those who implemented it only 1 in every 6 used the configuration that protects their domains from email impersonation. This lack of protection allows cyber criminals to send emails to staff and donors on behalf of the charitable organisation, leaving them vulnerable to online fraud via email and leaving the organisations' brands at risk.

The charity sector in England and Wales has reported over £70Bn in annual income in 2016. This fact combined with a low level of protection makes UK charities and their donors potential targets to scammers.

The level of protection found in the UK charity sector is much lower than that of the private sector. Comparatively the public sector is set to show a strong increase in adoption since DMARC has been included in the digital guidelines by the National Cyber Security Center.

Key facts

- Fewer than 1% of UK charities have implemented email authentication with DMARC. Only 16% of the ones that have implemented it set it up to reject unauthorised emails, the rest only monitor such traffic but don't stop it.
- The Top 100 Charities shows a slight increase in adoption, up to 5%. However, none of these organisations have set DMARC to block unauthorised email. This could be due to fear of blocking valid email services, however this leaves them unprotected against phishing attacks that start with email impersonation.
- Several organisations in England and Wales have set up DMARC to full enforcement with no reporting mechanism in place. This gives them no visibility on legitimate communication being blocked due to misconfiguration of the email services.

INTRODUCTION

The UK government, recognising the critical importance of cyber security in the country, created the National Cyber Security Centre (NCSC) in October 2016. One of its first activities has been to include in their digital guidelines to all government agencies the need to protect their domains from phishing and email impersonation by using DMARC (Domain-based Message Authentication, Reporting & Conformance). This email security protocol protects a domain by validating authorised emails and by blocking and reporting unauthorised emails that use a domain. The NCSC also recommended that the private sector abide to this guideline.

The spectrum of phishing attacks range in techniques, including the use of similar domains, and the use of masks to impersonate their victim's domains. The most sophisticated attacks in this range send emails using the actual domain of the organisation. DMARC protects against this specific attack, blocking unauthorised emails that use an organisation's domain. A comprehensive anti-phishing protection includes the implementation of DMARC as well as other anti-phishing measures.

One of the first government agencies to adopt DMARC has been HMRC, which was the highest impersonated brand in the UK. After HMRC implemented DMARC on their domains, they closed 2016 having blocked 300 million phishing emails.

This prompted OnDMARC to look at the charity sector and analyse more than 78,000 domains from UK organisations. This analysis is aimed at understanding how many of them implement email authentication protocols to protect their organisations, their users and their donors from cyber-attacks. The charities included in this study are from:

- England and Wales (71,700+)
- Scotland (5800)
- Northern Ireland (960)

This analysis found that only less than 1% of those organisations are protected from email impersonation.

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting & Conformance) was developed by online industry leaders as part of a global effort to make Email reliable again. Currently almost all email servers accept it as a way to validate that the sender of an email is authorised to do so. DMARC is a standard that prevents spammers from using your domain to send email without your permission — also

known as spoofing. Spammers can forge the “From” address on messages so the spam appears to come from a user in your domain

DMARC ensures these emails get blocked before you even see them in your inbox. In addition, DMARC gives you great visibility and reports into who is sending email on behalf of your domain, ensuring only legitimate email is received.

DMARC can be configured to only monitoring mode or to a mode that blocks unauthorised emails. It’s important that organisations get to the blocking mode as it’s the one that protects against phishing attacks.

Email Security protocols SPF and DKIM

DMARC uses the results of two other protocols SPF and DKIM, to validate the authenticity of an email.

SPF stands for Sender Policy Framework and contains a list of services that are authorised to send emails on behalf of an organisation. Emails that have not been sent by any of these services will fail the SPF validation.

DKIM stands for DomainKeys Identified Mail confirms that the content of the email hasn’t been tampered with. It does so by using an encryption key that also validates that the sending server who signed the email is authorised to do so.

Deliverability

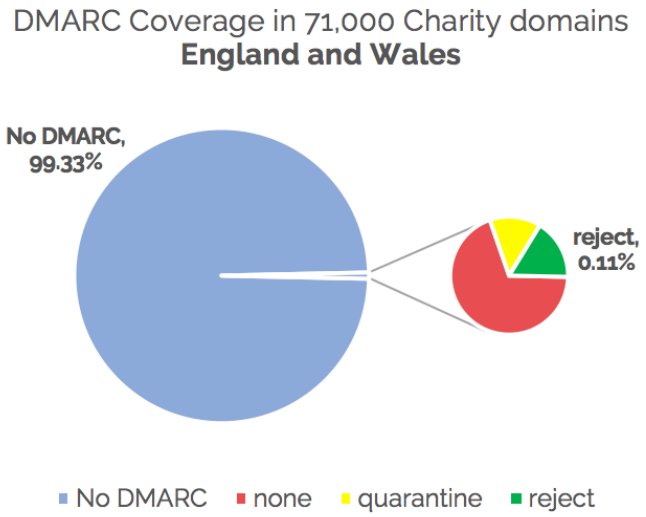
DMARC not only allows a domain to be protected against email impersonation but it also increases the capability of an email campaign to reach the inbox of their subscribers. Legitimate emails such as fundraising campaigns have a higher probability of getting delivered to their destinations because such emails will be treated as authentic by the receiving email servers.

ADOPTION OF DMARC IN THE UK CHARITY SECTOR

England and Wales

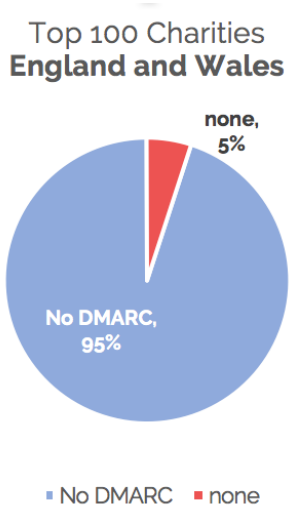
OnDMARC analysed more than 71,000 domains for Charities registered in England and Wales. The implementation of DMARC in this group is extremely low with less than 1% covered.

Only 16% of that 1% who have implemented DMARC have set it to enforce the rejection of unauthorised email. This means that the other 84% have implemented DMARC but are still allowing potentially malicious email to reach the mailboxes of their victims.



Less than 1% of charities implement DMARC. 0.11% set their policy to reject malicious email

This analysis also found that the group of charities which is blocking unauthorised emails have full protection in place, however several of them have not set up a mechanism to receive reports and have no knowledge of instances where they could be inadvertently blocking email from authorised sources. This could be harming their capability to get their messages to their partners and donors.



To understand how the situation is represented in the biggest organisations in the sector, OnDMARC looked at the Top 100 Charities ranked by fundraising income and found that the DMARC adoption is slightly bigger with 5% of those organisations having implemented DMARC but none of them have implemented their policy to reject unauthorised emails.

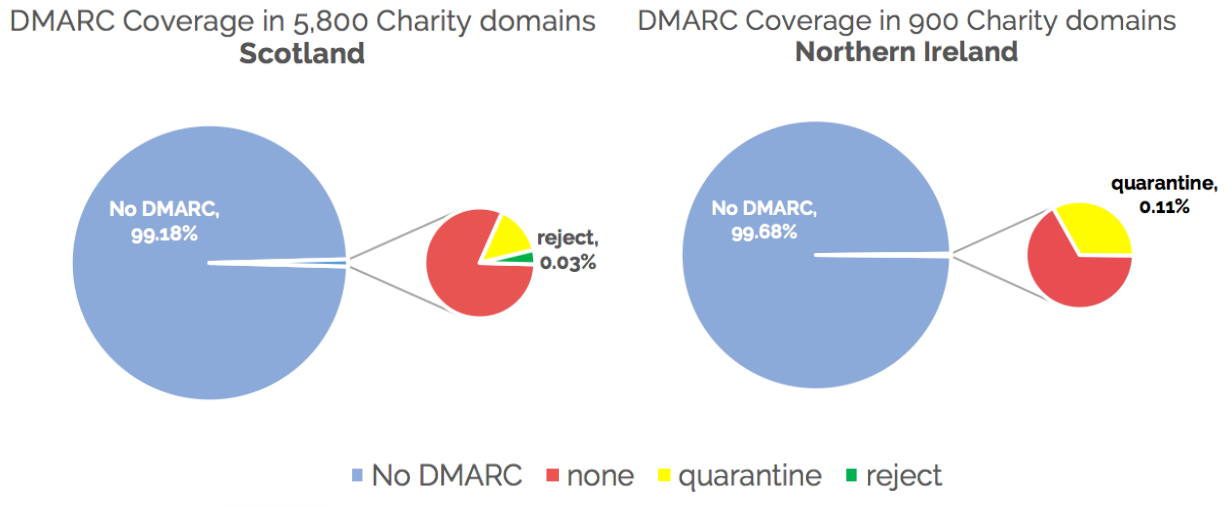
This could be due to the fact that those organisations do not have the tools and information to confidently set up DMARC to reject of unauthorised email without fear of blocking authentic communications with people in their ecosystem (donors, volunteers, employees, subscribers, etc).

Scotland and Northern Ireland

This study found similar numbers for Scotland and Northern Ireland as the ones for England and Wales. Less than 1% of adoption of DMARC and an even lower implementation of the rejection policy.

In Scotland, we found that 48 organisations implemented DMARC and only 2 of them set it to reject unauthorised email.

In Northern Ireland only 3 charity organisations implemented the DMARC protocol but none of them set it to reject unauthorised email.



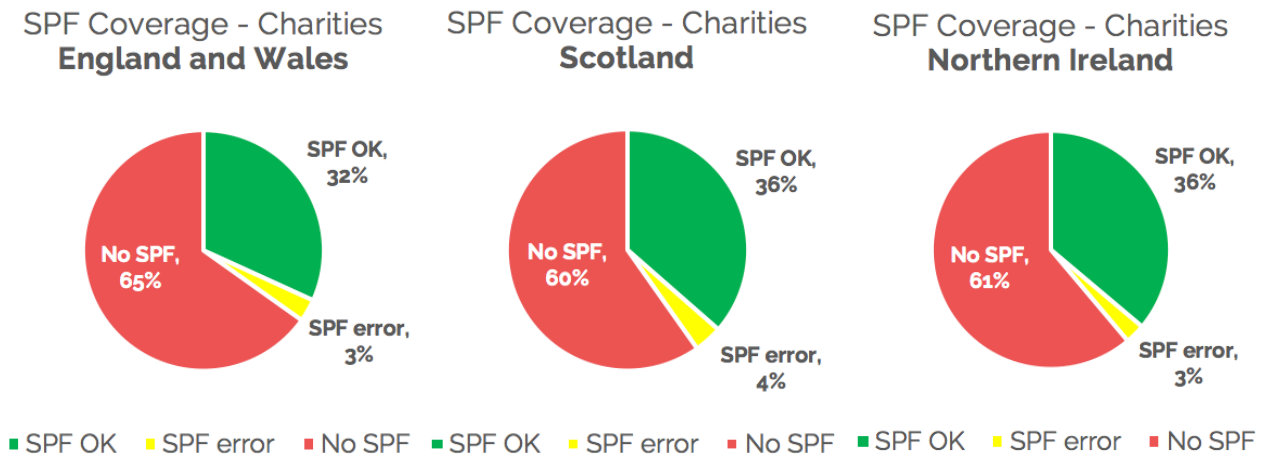
ADOPTION OF SPF IN THE UK CHARITY SECTOR

In the same analysis OnDMARC looked at the presence of the SPF configuration in the charity domains.

At the conclusion of the study we found a very low rate of implementation of SPF. The study also showed a high rate of domains with misconfigured or non-existent SPF records, showing that in several cases the implementation of SPF can be complicated, necessitating a tool that can make it more straightforward.

Across the 3 groups of charity domains that we analysed we found that just over 30% of them had implemented the SPF validation protocol and around 3% to 4% of them had an error in their implementation.

The errors that this study found are only related to incorrect syntax in the SPF records, but we cannot establish that the re valid records were correctly configured to cater for all the email services used by each charity. Charities with incomplete implementations in addition to the ones with errors and with No SPF records are weakly positioned to ensure their communications get to the intended recipients with confidence.



METHODOLOGY

OnDMARC produced this report by making an analysis of over 78,000 domains from the UK charity sector. The analysis was conducted in December 2016 and it looked specifically in the adoption of the DMARC and SPF email authentication protocols.

In our analysis, we checked a number of factors for each of the domains analysed, this allowed us to understand adoption rates, configuration type and configuration errors.

The analysis was done looking at public data in the DNS records for each primary domain under the control of each charity to categorise their DMARC and SPF implementations.

The data of the charity domains was gathered from the information available in the websites of the Charities regulators in the UK.

- England and Wales - domain names data available from the website of the Charity Commission for England and Wales. We found that from the 150,000 charities only 71,000 had submitted valid domains that we could analyse. https://www.gov.uk/government/organisations/charity-commission

- List of Top 100 Charities in England and Wales as reported by Charity Financials - Feb 2016 http://secure.charityfinancials.com/reports.aspx

- Scotland - domains data available from the Scottish Charity Regulator website: http://www.oscr.org.uk/

- Northern Ireland – domains data is available from the website of The Charity Commission for Northern Ireland: http://www.charitycommissionni.org.uk

About OnDMARC

OnDMARC specialises in helping companies implement and maintain their email authentication policies. The solution provides clear actions to implement your DMARC records and a quick and hassle-free way to reach full protection against email impersonation attacks.

OnDMARC is part of Red Sift, a provider of a platform for creating applications that can compute live streams of data.