Protect your brand from phishing emails by implementing DMARC[1]

Message from the Certified Senders Alliance supported by AOL, Microsoft and Google

In the following article we want to clarify why marketers should implement DMARC as protection against phishing. Statements and interviews from relevant international ISPs support our point of view. We have also put DMARC in context of the technical delivery of emails for those who want to understand the full technical picture.

Is phishing relevant today? Which companies are affected?

With the rising number of emails and new methods employed by spammers and phishers, ISPs are continuously facing the challenge of evaluating whether to accept or reject an email. According to Kaspersky Labs, "spam becomes really problematic as soon as it is used to spread malware or gets "infested" with phishing. In the first quarter of 2015, the Anti-Phishing System was triggered 50,077,057 times on the computers of Kaspersky Lab users. This is 1 million times more than in the previous quarter."[2] Other reports emphasize that there is indeed a growing risk to business data from email-based malware.[3]

"42% of people surveyed feel that their trust in a brand would be greatly reduced if they received a phishing email claiming to be from that company."[4]

Most attacks focus on banks, online stores, and electronic payment systems. However, this is not the whole story. In Q1 2015 Kaspersky included a new category "Delivery companies" in their rating which has recently demonstrated noticeable growth (+0.04). DHL, one of the companies in this category, was among the Top 100 organizations most

1 DMARC = Domain-based Message Authentication, Reporting and Conformance of messages (https://dmarc.org)
2 https://business.kaspersky.com/spam-and-phishing-in-q1-2015-banks-and-banking-trojans/4113/
3 http://pages.cyren.com/TrendReport_2015Q1.html?utm_campaign=ALL_ALL_2015_Q1_Trend_Report&utm_medium=press_release&utm_source=press_release
4 https://www.cloudmark.com/en/press/reputation-of-uk-brands-dramatically-affected-by-phishing-attacks-according-to-survey-commissioned-by-cloudmark

often attacked by phishers.[5]

"Apart from the aforementioned most attractive industries, every brand with a good reputation based on consumer trust is a potential target. Companies which invested in branding face the challenge that their trusting customers receive emails asking for personal data or even payment details" says Alexander Zeh, Engineering Manager in charge of technical certification at the CSA.

How can DMARC protect brands from phishing attacks?

With DMARC and the related technologies Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) a brand has the opportunity to make its emails clearly identifiable for an ISP and, at the same time, determine how the ISP should treat emails which only pretend to originate from the brand. Consequently, phishing emails can be reliably identified by the ISPs and get filtered before reaching the recipient. In contrast to classical approaches which are based on content filters, a single phishing email can already be identified and blocked.

Why international ISPs want marketers to implement DMARC

AOL:

"DMARC allows more security as phishing is a hard problem to solve. A very high percentage of phishing mail is still delivered to real users. Using DMARC, leveraging its reporting and policy capabilities helps to reduce spoofed mail to almost zero.

DMARC works today so implement it today, improve deliverability and maintain a healthy relationship with the ISP community. If you're not doing it, you're competing with bad guys to not look like a bad guy."

Marcel Becker
Director Product, Mail
AOL

5 https://business.kaspersky.com/spam-and-phishing-in-q1-2015-banks-and-banking-trojans/4113/

Microsoft:

"As email threats and spear phishing grow, every business should make email authentication, and especially DMARC, a priority to help protect their consumers, their employees and their brands. Authenticating your mail, and having a strong DMARC policy helps protect you from reputation damage caused by others spoofing your domain. As major receivers increasingly rely on domain-based reputation, this is crucial for the continued deliverability of your email."

Terry Zink
Program Manager
Microsoft Corporation

Google:

CSA: *"Should senders implement DMARC in your opinion? If yes, why?"*

Sri Somanchi: *"Yes, it´s an easy way to make sure that their domain (and brand) is resilient to spoofed mail and thereby protects their users from getting phished."*

CSA: *"Can senders count on a better deliverability after having implemented DMARC? Which value do you see for senders, how does Google treat senders who have not implemented DMARC?"*

Sri Somanchi: *"While deliverability and DMARC do not have a direct co-relation, the identity protection offered by DMARC helps augment user trust in a sender's email and thereby preventing users from mistakenly marking the sender's good mail as spam. DMARC also makes it easier for the receivers by not letting spoofed mail corrupt the sender's reputation."*

Sri Somanchi
Google

Conclusion:

By implementing DMARC marketers can ensure that their identity does not get misused, which could cause major damage to ISP infrastructure and brand reputation resulting in a loss of trust of customers in the respective brand. Marketers in charge of email marketing should address the topic of implementing DMARC with their email service provider.

The Certified Senders Alliance is offering information and support on this topic at the CSA Summit taking place April 20th-22nd 2016 in Cologne, Germany.

Annex

How DMARC fits into the ISP`s antispam and anti-phishing toolkit

Let´s look at the email value chain. There is always a company (brand) that wants to deliver a message to a receiver. Sometimes the brand has an ESP which takes care of the technical delivery. The ISP which owns the mailbox of the receiver needs to decide whether to accept or reject the email.

The outgoing mail server from the email service provider connects to the inbound mail server from the ISP. The ISP sees the IP address of the connecting server.

There are different levels of communication between servers along the email value chain. The higher the level, the more sophisticated the communication and the higher the probability of getting delivered, respectively protected against phishing.

1. Basic communication: The "envelope" check:

   The mail server of the ISP checks in the **D**omain **N**ame **S**ystem if the IP address really belongs to the host domain name, as stated in the HELO. Even if this check is successful, there are problems for the ISPs involved regarding the clear identification of the sender: IP addresses can be passed on or shared, so there could be many brands which send or have been sending from this IP. Additionally, the host domain name could be fake.

   Conclusion: ISPs do not rely on this basic form of communication when deciding whether to deliver an email or not as the IP address could be shared or fake. The latter goes for the host domain name as well. Furthermore, they have not yet

received information on the mailfrom domain. **As a consequence, the email may not get delivered.**

2. Advanced communication: The "header" check:

   ISPs check the mailfrom domain of the email in order to find out who has actually written the email. However, one problem remains: The mailfrom domain can be misused by someone pretending to be the owner of this domain.

   Conclusion: ISPs do not rely on this advanced form of communication when deciding whether to deliver an email or not. **Thus, the email may not get delivered.**

3. Advanced communication with the **S**ender **P**olicy **F**ramework:

   The "envelope check" allows brands to list IP addresses in the DNS which are authorized to send emails with their mailfrom domain. The listing of IP addresses can also be handled by the ESP as described above. Brands may face an organizational challenge to identify the entire list of IP addresses, but at the same time manage to prevent any misuse of a mailfrom domain at an early stage. SPF failure reporting is a required CSA admission criteria.

   Conclusion: ISPs do not rely on SPF checks alone because a brand (mailfrom domain owner) which sends via the same (shared) IP as another one may misuse the other brand´s identity. This potential risk increases with the number of mailfrom domain sendings via the same IPs. **Consequently, the email may not get delivered.**

4. Advanced communication with the **D**omain **K**eys **I**dentified **M**ail

   The "header with digital signature" check: A digital signature of the brand or ESP allows ISPs to prove that the sending domain is really what it pretends to be, resulting in a Domain Keys Identified Mail. There are two keys which need to be generated in order to be able to send DKIM signed emails: A private key, which is used to generate the signature, and a public key, which allows the ISPs to check the signature. The ESP generates both keys and keeps the private key. The public key needs to be published by the brand in the DNS. Alternatively, the brand can give a domain- or subdomain delegation to the ESP which can then handle the publication of a public key.

   Conclusion: ISPs rely on DKIM as it allows clear identification of a brand, however,

keys may still be misused. DKIM procedure is a required CSA admission criteria. Only DKIM and SPF together allow the ISPs to make a decision regarding delivery or non-delivery based on the real mailfrom domain and related IP address. If DKIM and SPF are not set up or checks fail, the ISP can only make a decision upon IP reputation with the related challenges in 1. **As a consequence, the emails are likely to end up in the spam folder.**

5. State of the Art communication with DMARC:

   The "how to handle emails where DKIM or SPF fail?" DMARC is a policy which can be published by the brands in the DNS of the mailfrom domain. It advises the ISP on how to handle emails where DKIM or SPF checks fail. Possible options: None (=deliver), quarantine and reject. Brands receive a report every time a DKIM or SPF check fails, among which the daily aggregated report is the most common one. Reasons for failure may occur if the mailfrom domain owner partly sends by himself (without SPF & DKIM) and partly via an ESP. This may result in confusion on the ISP´s side if the mailstream is fake and will therefore be blocked. In a nutshell, the report allows brands to:

   - protect their customers by identifying potential phishing and related sources
   - analyze their infrastructure and switch off IP-addresses without SPF and DKIM
   - set up DKIM and SPF for IP addresses which belong to the brand and will disappear in future reports

   In its detailed legal report on DMARC, the eco competence group Email recommends German ISPs to send aggregated reports.

Authors: Julia Janßen-Holldiek, Manager ISP Relations & Business Development