RED SIFT

Email Security for the Retail Sector

Exploring the threats and opportunities for retailers in today's email landscape

We put this report together not only to highlight the current state of email insecurity across the retail, and e-retail, sector but to show how easily the situation can be remedied. Through implementing the foundations of email security such as SPF, DKIM and DMARC retailers can protect themselves and their customers from email impersonation fraud and boost email deliverability rates.

We hope you find it both interesting and useful!

Introduction

Despite constant reports of its demise, email is alive and well. In fact, it's growing at a rapid pace. In 2020, it's estimated that more than 300 billion emails were sent every day. That figure is expected to reach 376 billion per day within the next few years, and analysts predict that nearly 4.5 billion people will be using the email channel by 2024.

In the retail industry, email is an integral part of doing business. Every day, hundreds of thousands of retail businesses worldwide rely on email for their internal and external communications. But the very prevalence of email makes it an attractive target for cybercriminals looking to steal money or data — or both.

Email integrity and brand reputation are more important than ever, especially for retail brands. In this paper, we will explore the email security threats facing retailers and the measures they should take to avoid falling prey to breaches and fraud. We'll also look at trends in email security — not only to highlight the state of email across the retail sector, but to show how measures like DMARC and BIMI can improve the status quo.

Retail at a glance

$25 Trillion
generated worldwide from retail sales annually

19%
of those sales (about $4.5 trillion) are made online

1 Million+
retailers operate across the US

15 Million+
people are employeed by US retailers

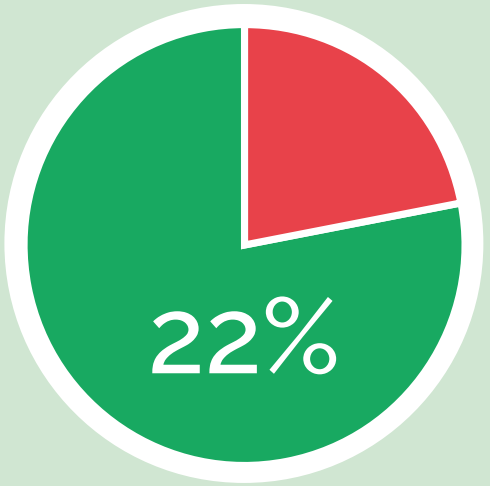
Retail generates 5.5% of the total US GDP

Cybercrime:
A Major Concern for Retailers

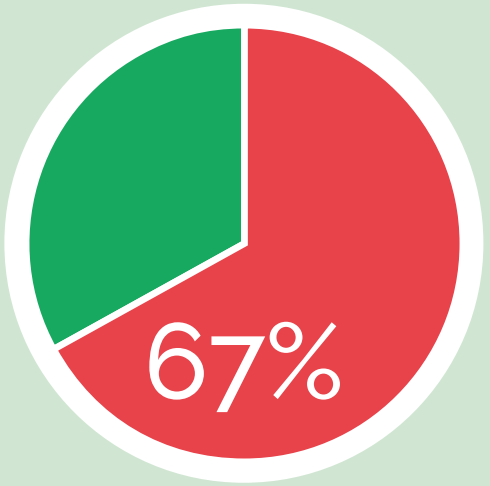
There's no question that cybercrime is a costly problem. A 2020 report from McAfee and the Center for Strategic and International Studies (CSIS) found that global losses from cybercrime now total more than $1 trillion — just over one percent of global GDP. This represents an increase of more than 50 percent since 2018.

While all businesses are at risk for fraud and data theft, the retail sector is particularly susceptible to cybercrime. In fact, 24% of attacks target retailers, at a cost of more than $30 billion each year. Retail accounted for just 18% of cyberattacks in 2018, so this threat is clearly on the rise.

While these numbers are staggering, they don't take into account the downstream impact of a security breach. Retail businesses rely heavily on consumer trust, and reputation is paramount. A high-profile cyberattack can lead to long-term loss of confidence, especially if it involves Personally Identifiable Information (PII) and financial data. In the US, 22% of people will stop doing business with a company that has been hacked and two-thirds trust a company less after a breach.



22% of people won't do business with a company that's been hacked



67% of people trust a company less after a data breach

It's difficult to imagine a more vulnerable target than the retail sector and its customers. Retailers are in constant communication with their customers — especially via email — opening up the potential for phishing and spoofing. And retail databases frequently house sensitive customer data like email addresses, phone numbers, and credit card information. It's no wonder the retail sector accounts for nearly a quarter of all breach incidents — more than any other industry.

Phishing/Social Engineering is the method of compromise in half of all attacks

50%

Retail is the most targeted industry, accounting for nearly a quarter of all breaches

24%

Trustwave's 2020 Global Security Report shows that phishing/social engineering is the top method of compromise, accounting for 50% of all attacks. The second most common method, malicious insiders, was present in just 11% of attacks. This demonstrates a clear need for retailers to shore up their email security, as it is by far their greatest vulnerability.

The High Cost of Cyber-Insecurity

Security is a business imperative in the retail industry. Customers must be confident that their sensitive data will be safe, and they must trust that retailers are taking appropriate security measures.

On the regulatory side, retailers are legally responsible for safeguarding customers' personal information and payment details. They are also required to disclose any data breaches that occur — a situation that can jeopardize a retailer's reputation as news of a data breach goes public.

Today's retailers also risk significant financial penalties for lapses in data security. For example, the UK's far-reaching GDPR imposes fines of up £20m (about $28m or €23.5m) or 4% of annual revenue for each data breach. With more cybercrimes being reported than ever before, the industry faces an uphill battle in combating this type of crime.

Ultimately, retailers need to consider which consequences from a breach or hack matter most. Every retailer has a different level of risk tolerance. For some, reputation and consumer trust are more important than financial loss. Others may value the bottom line over possible damage to their brand.

Isn't GDPR a UK law? Yes. However, its requirements apply to any company doing business with EU citizens. Given the global nature of retail commerce, all retailers would do well to comply with GDPR.

£20m

or 4% of annual turnover

Under GDPR, businesses may be fined £20m (about $28m or €23.5m) or 4% of annual revenue for a data breach.

Top Email Threats Facing Retailers

Email fraud comes in several forms, but its goals are always the same: to steal money, to steal data, or to bring business operations to a halt. Whatever the circumstances, one thing is certain: the reputation of the target organization is at risk.

Before a retailer can take effective action against email fraud, it's useful to understand how it happens and what it might look like.

How

Sender fraud happens when the sender's domain (e.g., retailer.com) has a critical vulnerability which is open to exploitation. The domain can be spoofed, so emails can be sent by a scammer using the '@retailer.com' email address. These fraudulent emails look authentic, and there's no simple way for the recipient to distinguish a legitimate email from a fake. This is the most technically sophisticated type of email scam, as it involves both human and digital deception.

Recipient fraud is a less sophisticated type of fraud. Instead of impersonating a domain, the scammer purchases a similar domain name (e.g., 'ret4iler.com'). The fake email address can easily be identified by an observant recipient, and this fake email address is unlikely to be automatically added into an existing contact.

What

Business Email Compromise (BEC)/Email Account Compromise (EAC) is a tactic where scammers target individuals (for example, the accounts team) and manipulate using social engineering techniques. One common trick is to send an authoritative-sounding email that looks like it came from the CEO or other executive, with instructions to pay false invoices or share data.

CEO fraud is an attack levied against senior executives within the business. Scammers send emails to senior leaders with the authority to initiate payments, purporting to come from a known or trusted sender. The goal is to induce the targeted individuals to reveal confidential information or authorize the transfer of funds.

Prevention or Cure?

While some retailers have managed to recover from cyberattacks, a positive outcome is not guaranteed. Stolen money can be recovered or replaced, but stolen data creates a whole host of issues. Fines, reputational damage, and loss of consumer confidence may spell the end for some firms.

Instead of mitigating their loss after the fact, retailers should take steps to prevent cyberattacks from happening in the first place.

There are some simple solutions for combating human-based fraud, by educating employees about email threats and conducting periodic tests to help them identify and avoid phishing attacks. Retailers can also take steps to educate their customers on email fraud – for example, with a side-by-side comparison showing their legitimate email versus commonly spoofed elements in a fraudulent email.

For sender fraud, prevention lies in a technology-based solution. Many organizations will assume that their existing email systems will do the job of protecting them, but anti-spam and anti-malware products can't stop email impersonation.

An email protocol called DMARC (Domain-based Message Authentication, Reporting, and Conformance) provides some measure of relief for retailers facing these more sophisticated email threats.

Understanding DMARC

DMARC is a globally recognized email authentication standard that helps protect email senders and recipients from spam, spoofing, and phishing attacks. DMARC is able to accurately validate emails, block phishing attacks, and help recipients determine whether email is coming from a legitimate source. It is widely used by government bodies, Fortune 500 companies, and more.

Adoption of DMARC is growing rapidly. As of December 2020, more than 2.7 million companies worldwide have DMARC records — up from 1.9 million at the end of 2019 and 630,000 at the end of 2018.

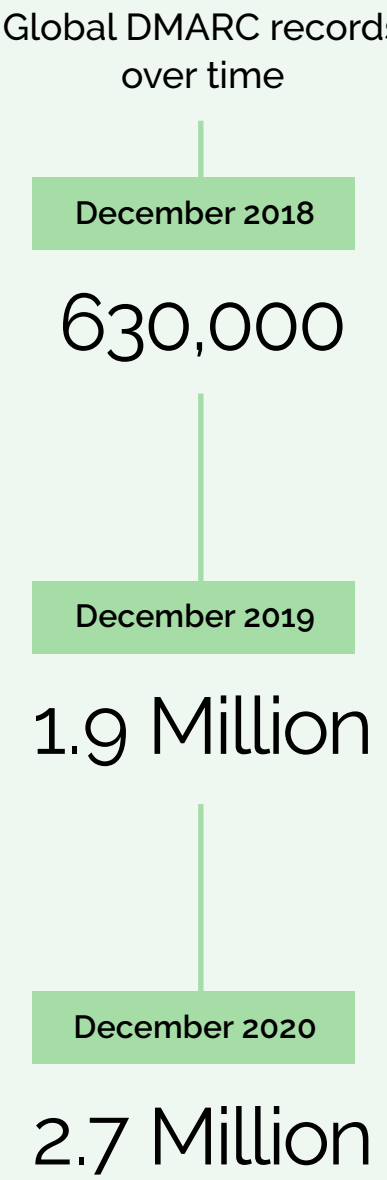
Under DMARC, there are three basic "policy tags" that allow senders to define how email from their domain should be handled. Companies that have at least partially implemented DMARC protocols will have the following tags in their DMARC record:

P=reject: This indicates full DMARC protection; messages that fail authentication are rejected and will not reach the inbox.

P=quarantine: This indicates partial DMARC protection; messages that fail authentication are quarantined (typically marked as spam/junk).

P=none: This indicates limited DMARC protection, often called "monitoring" mode; messages that fail authentication will be reported, but no additional action is taken.

Companies that haven't yet taken steps toward implementing DMARC protocols have no published DMARC record.



The State of Cybersecurity in Retail

It is difficult to judge a company's cybersecurity efforts from the outside, but one simple option is to look at their adoption of basic security protocols. In March 2021, Red Sift analyzed the DMARC records of nearly 300 global retailers to get a sense of how the retail sector is approaching cybersecurity.

Cybersecurity in 2021:
90% of global retailers are vulnerable to email fraud

Red Sift conducted a unique survey of 287 top retailers worldwide. Among this sample, only 17 businesses had full DMARC protection in place, and 12 had partial protection. This reveals a critical vulnerability for 90% of retailers — and a clear opportunity for scammers.

The results are as follows:

DMARC Status	Explanation	# of retailers	% of retailers
P=reject	Full protection	17	6%
P=quarantine	Partial protection	12	4%
P=none	No protection, reporting only	149	52%
N/A	No DMARC record published	109	38%

2021 DMARC Status
of the top global
e-commerce & retailers

- Reject **6%**
- Quarantine **4%**
- Reporting only mode **52%**
- No DMARC in place **38%**

As these numbers demonstrate, getting started with DMARC implementation is the easy part. Moving from p=none to p=quarantine or p=reject is much trickier.

Gathering DMARC reports in the p=none stage is fairly straightforward, whereas analyzing them and configuring your email sending services accordingly is not. Without AI-powered technology to collect and interpret the dense XML reports, retailers can get lost in a maze of confusing detail. Ultimately, this means the project often gets pushed to the back burner while it's only partially completed.

It's also not unusual to see errors and failures creep into some retailers' DMARC implementations. IT teams may accidently get the code wrong in their DMARC record, so the protocol doesn't function properly or exceeds the 10-lookup limit for resolving each SPF record (a process used by mailbox providers on receiving each new message). As a result, legitimate email will randomly fail authentication and miss out on reaching the intended inbox.

Without AI-powered technology, retailers can get lost in a maze of confusing detail when implementing DMARC.

DMARC and Email Deliverability

DMARC has been widely adopted by the world's largest mailbox providers, including Google, Apple, Yahoo, Hotmail/Microsoft, AOL, and more — accounting for nearly 80% of consumer inboxes worldwide. Many of these providers have been using DMARC since its inception in 2012 to protect their users from fraudulent email.

As the challenge of email deliverability continues to increase, it's more important than ever for retailers to ensure their emails are seen as legitimate. Today one in six emails won't reach the inbox — and each failed email represents a missed opportunity to connect with subscribers, build a relationship, and ultimately convert a sale. Implementing DMARC is a clear signal to mailbox providers that your email poses no threat to their users.

Recently several countries have made DMARC implementation mandatory or recommended for national government organizations. Although not directly applicable to retailers this shows how DMARC is viewed as part of the foundations of good cybersecurity practice.

- U.S. Binding Operational Directive 18-01 (2017) Mandated all federal government domains to establish a DMARC reject policy within a year

- The U.K. Government Digital Service (GDS) security guidelines (2016) All UK government domains, and suppliers, must publish a DMARC policy and set it to reject

- Australia's Malicious Email Mitigation Strategies Recommends that all organizations—federal or otherwise—establish a DMARC policy and set it to reject

- The Netherlands' Standardization Forum mandated that Dutch government organizations implement a DMARC reject policy by the end of 2019

1 in 6

emails fail to reach the inbox.

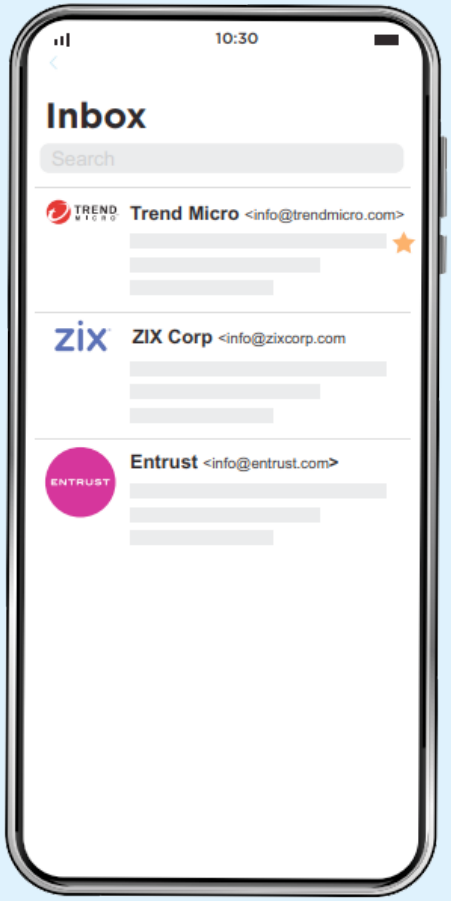
BIMI: A New Layer of Email Authentication

For retailers who have already implemented DMARC, there's a new authentication tool that can help to increase sender credibility among email recipients. BIMI (which stands for Brand Indicators for Message Identification) allows senders to display their trademarked logo as part of each authenticated email.

BIMI works as part of a comprehensive email authentication solution. Implementation requires the brand to first:

- Implement DMARC protocols ("p=reject "or "p=quarantine")
- Acquire a Verified Mark Certificate (VMC) for their logo

VMCs are innovative digital certificates, developed by Entrust in collaboration with BIMI. VMCs verify a brand's trademarked logo and confirm their business identity by performing a high assurance verification check. A VMC can be issued only after the brand implements DMARC (p=reject or p=quarantine). Once everything is confirmed and configured correctly, the sender's emails can automatically display their logo in a secure, interoperable way.



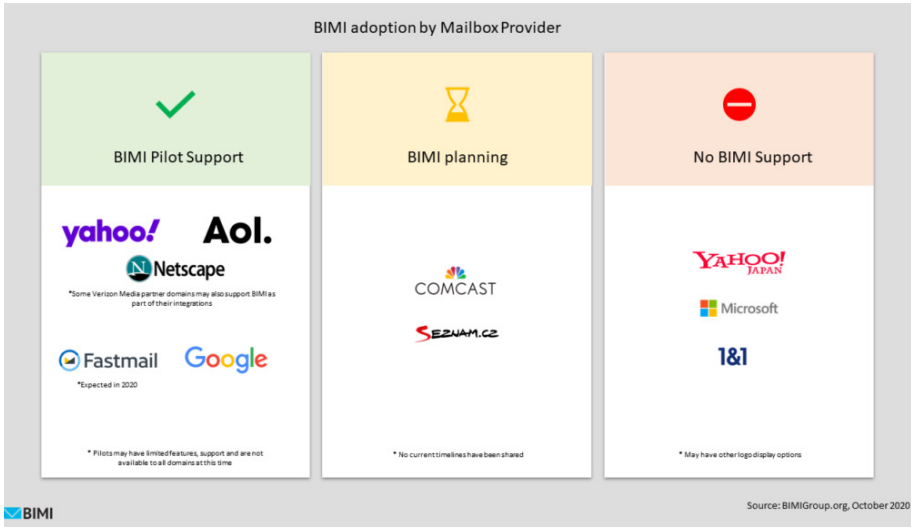
With BIMI, the email user sees the sender's logo alongside their message, giving a clear visual signal that the email is legitimate.

The Benefits of BIMI for Retailers

Implementing BIMI provides significant benefits for retailers. This measure allows them to:

- Display their trademarked logo on email messages, increasing brand visibility and brand recognition in the inbox
- Deter email fraudsters with email authenticity, which enables them to display their trademarked logo
- Improve email deliverability (in conjunction with DMARC authentication)

While BIMI is still relatively new, adoption by mailbox providers is on the rise. Top mailbox providers currently in the beta phase of supporting BIMI include Gmail, Yahoo, and AOL.



In addition, early results indicate that displaying a brand logo may increase open rates by as much as 10%. These clear and substantial advantages may be just the incentive retailers need to implement DMARC on a larger scale.

Why the Retail Sector Needs DMARC and BIMI

There's no question that cybercrime is a significant threat to retail companies. With more and more online interactions between retailers and customers, it's critical to ensure that email communications are safe and trusted.

Here are a few reasons why the retail sector needs to improve adoption of protocols like DMARC and BIMI:

Email deliverability

Top mailbox providers like Gmail, Apple, Yahoo, and Microsoft have become increasingly protective of their users and the overall inbox experience. DMARC ensures that emails are reliably authenticated, leading to higher deliverability rates.

Company reputation

Retailers that are frequent victims of email phishing and spoofing may suffer considerable damage to their reputation. Email scams attract negative press, and the target organization often bears the blame.

Consumer trust

Companies that fail to take precautions to prevent email fraud are likely to be considered less trustworthy. Customers may not trust email that appears to come from such organizations and may be hesitant to use email to communicate with them. Long term, this could derail relationships and damage the firm's bottom line.

Supply chain security

Often retailers don't look outside their own organization when it comes to cybersecurity. However an insecure supply chain can provide an easy access point for attackers. Ensuring that all partners and suppliers have secured their email domains can reduce the threat of attacks.

Financial security

Finally, and perhaps most importantly, email fraud can result in serious financial penalties. Now that GDPR is fully in force, the retail sector must ensure compliance with all applicable data privacy and security laws. The cost of data theft continues to escalate, but adopting DMARC could save an organization thousands — if not millions.

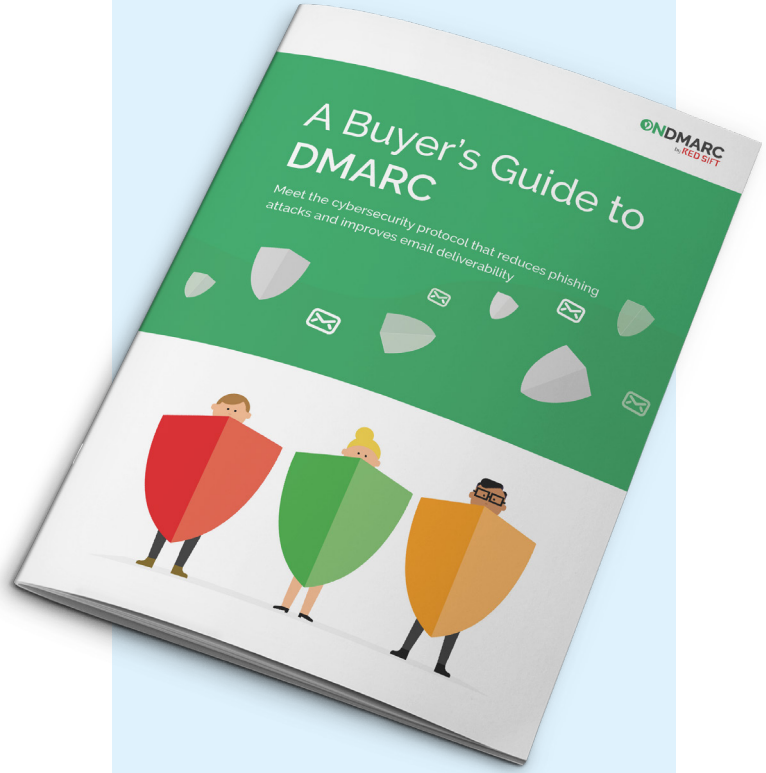
Finding the Right Partner

For retailers, email integrity and brand reputation are critical — but you don't have to go it alone. There are a number of services available to help retailers as they begin their journey toward full DMARC protection. These range from implementation packages and managed services to ongoing customer support through helplines or automated bots. Find the one that best meets your needs and you'll be well on your way.

As you search for a DMARC provider, make sure you consider all the essentials. What are their security accreditations? Are they using the p=reject policy themselves? What do existing customers think? What does their roadmap look like? What support and services can they provide you?

Be sure to consider your internal teams, as well. Gaining executive buy-in for DMARC can be tough, but there are resources available to help you educate key decision makers within your organization, such as Red Sift's DMARC Buyer's Guide. You'll also want to coach your employees on how to identify a phishing email and what to do if they receive one. A good DMARC provider can advise you on where to start.

Whether you're looking to chat with experts about DMARC or need some guidance on making your case to decision makers, we'd love to help. We'll offer honest, impartial advice and help you get DMARC-ready.



If you need some guidance on making your case to decision makers, we'd love to help!

RED SIFT

Methodology

In March 2021, Red Sift analyzed the DMARC status of 287 top retailers worldwide. To learn more about the results of individual retailers, please get in touch with the Red Sift team.

About Red Sift

OnDMARC is an email authentication product built on the Red Sift platform. Red Sift is a London based Platform as a Service (PaaS) offering businesses and individuals a secure way to collate, compute and visualize data from millions of individual signals to easily implement and optimize cybersecurity solutions.