EASYDMARC

DMARC for Informational Technology Industry:

risks and solutions

Table of Contents

Why is the IT industry in the risk group for phishing attacks?

Although high-tech companies are at the cutting edge of technological innovation, they are still vulnerable to attacks and exploits.
The fact is that the world can no longer advance without tech companies, and the ever-emerging threat of cybercriminals cannot be overlooked.
IT professionals and admins are the main targets of phishing attacks as they have many privileges, including having access to their companies' data. High-tech employees often use the latest (yet unsecured) mobile apps and devices, which can also be vulnerable to exploits.
The biggest threat to the IT industry is the loss of intellectual property (IP), which involves IP and personal information.

For example, suppose you are a large software provider with more than $1 billion in annual revenue. Hackers could invade your company's network and steal more than 100 million encrypted user credentials along with customers' credit card information..
Cybercriminals could also sell stolen source code for financial gain, a loss which would likely lower your company's long-term competitiveness.
According to the 2020 Phishing by Industry Benchmarking Report, technology companies have become the #1 most vulnerable industry among large organizations (of 1,000+ employees), with 55.9% of their users likely falling victim to phishing scams.

91% of all cyberattacks begin with phishing emails

Emails and other infiltration methods are designed to persuade staff to take steps that provide criminals with access to company data and funds.
Cybercrimes are carried out by phishing through the use of social engineering.
The rate of phishing attempts is increasing with the proliferation of leaked email addresses. 65% of targeted attack groups fall victim to spear-phishing as the major route of infection vector, and one in three 207 emails are phishing emails.

Cybercriminals primarily use phishing attacks to:

- Secure, detect and protect email spoofing of their domains Obtain login credentials for access to assets (an account, a server, a network, or similar).
- Steal other sensitive information, such as financial or personal information.
- Convince people to perform activities such as money transfers or the sharing of personal data against their self-interests.

Although there are other kinds of spear-phishing, email remains the most widely used vector with the worst potential consequences. Both private and corporate email addresses may be targeted depending on the goal of the attacker. Getting the target to trust the email sender is key to a successful spear-phishing attack. Data leaks of email addresses and passwords can provide easy access to cyberattacks. Once criminals have identified their targets, spear-phishing emails are sent to the relevant address. A phishing email sent from an email address belonging to an organization is often used for fraud and referred to as Business Email Compromise (BEC). In most BEC cases, fraudsters gain access to an organization’s email accounts. They then convince the targeted employee to transfer large sums of money to the criminal’s bank account, making use of the fact that the email comes from a trusted address within the organization.

Stay secure with DMARC

By implementing DMARC, brands reduce the probability that their domains are spoofed and used for phishing attacks on recipients. DMARC policies are designed to increase security from a simple reporting system to a strict policy where messages failing authentication are rejected without being delivered or seen by the intended recipient.

By adopting the DMARC standard, IT companies can:

- Secure and detect email spoofing to protect their domains
- Authorize and verify senders using their domain
- Reject emails sent by unauthorized senders
- Stop display-name and lookalike domains spoofing
- Monitor risky domains registered by fraudsters

The benefits of DMARC include:

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

DMARC policies:

P=NONE (GOOD)
None policy is the starting point for all DMARC implementations. By setting your policy to p=none, you will receive daily aggregate reporting from ISPs, with detailed information, such as authentication results of the email (number of messages which passed or failed authentication), and the number of messages seen using your domain name.
P=QUARANTINE (BETTER)

By setting your policy to p=quarantine, any email failing authentication will be routed to the spam/bulk/junk folder. **P=REJECT (BEST)**
The strictest policy level of DMARC is p=reject, which is used to block emails that fail authentication.

Does the IT industry lag in DMARC adoption?

The study conducted by EasyDMARC analyzed DMARC implementation across more than 216,000 domains in the IT sector.

After analyzing more than 216,000 domains controlled across EU and US IT companies, we found that 21,599 domains in the EU adopted DMARC by publishing a 17.4% reject policy. Meanwhile, 17,904 companies in the US IT sector adopted DMARC by publishing a 19.7% reject policy.
We found out that more than 50% of all analyzed domains have no DMARC policy in place, which means that more than half of EU and US IT companies leave consumer data vulnerable.

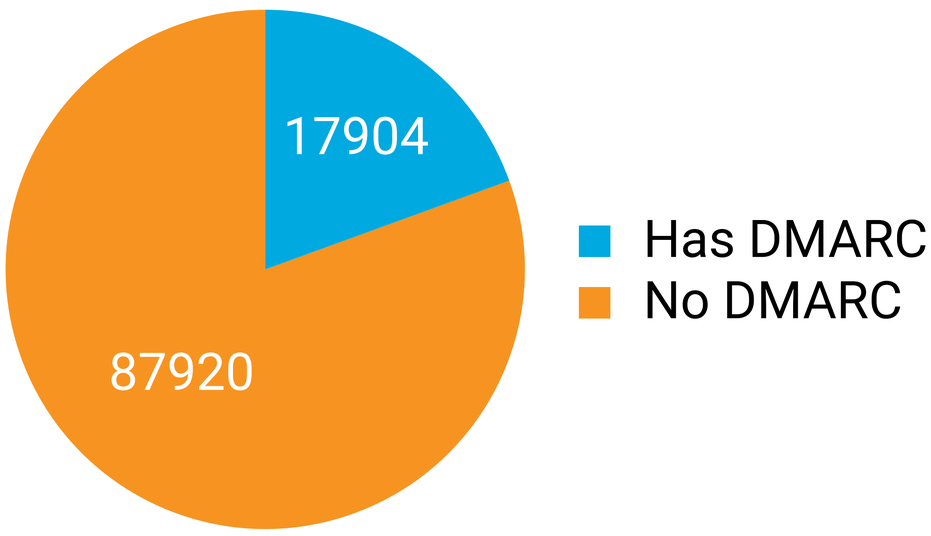
EASYDMARC
www.easydmarc.com
+1-888-563-5277
sales@easydmarc.us

DMARC adoption in the US

EasyDMARC analyzed 105,824 parent domains for IT companies operating within the United States.
The following graph shows the number of US IT company domains with overall DMARC adoption.

DMARC coverage for US IT companies

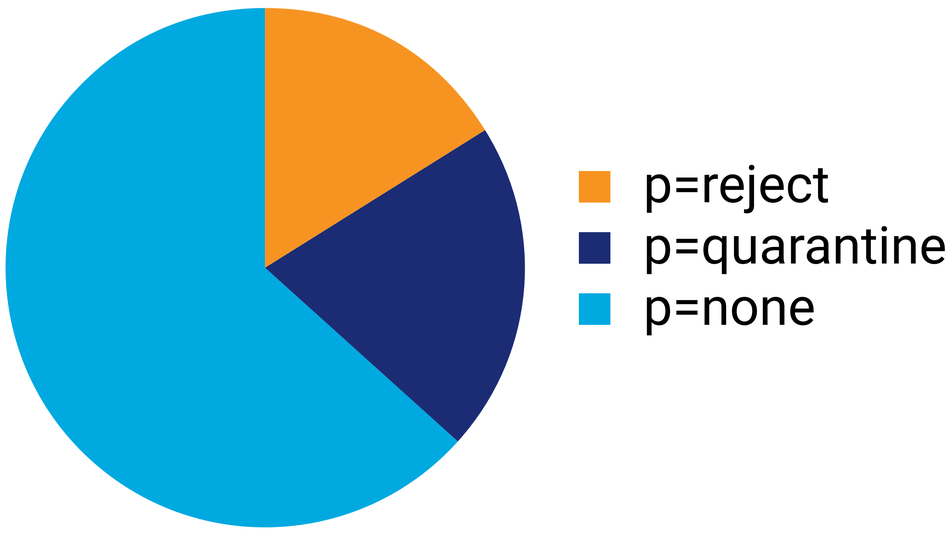
Legend
n = 105825 domains



DMARC adoption in US IT companies by policy

The following graph shows the proportion of each DMARC policy among US IT companies with active DMARC records at the end of 2021.

Us IT companies DMARC Adoption



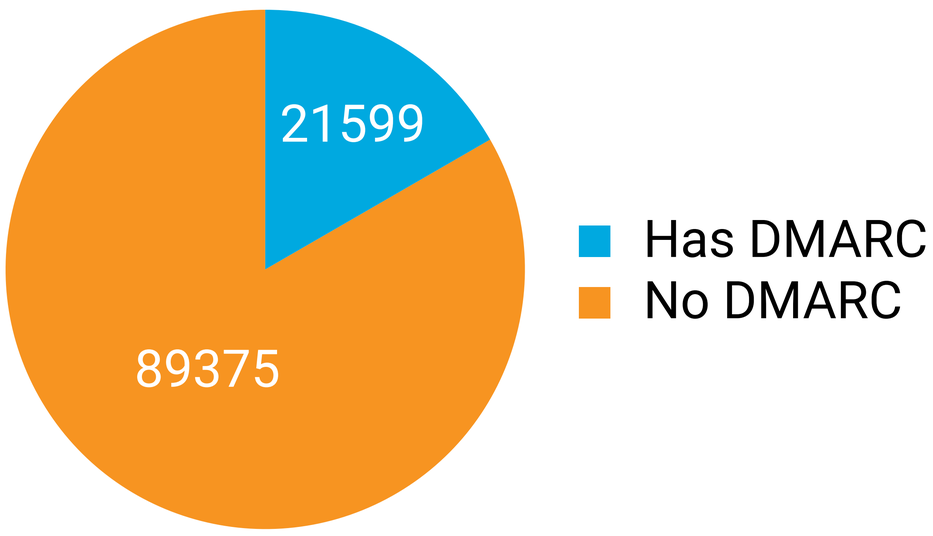
Even among US IT companies that have adopted DMARC, more than half still haven't reached "p=quarantine" and "p=reject" policies.

DMARC Policy mix in November 2021

DMARC adoption in EU

EasyDMARC analyzed 110,974 parent domains for IT companies operating within the European Union.
The following graph shows the number of EU IT company domains with overall DMARC adoption.

DMARC coverage for EU IT companies

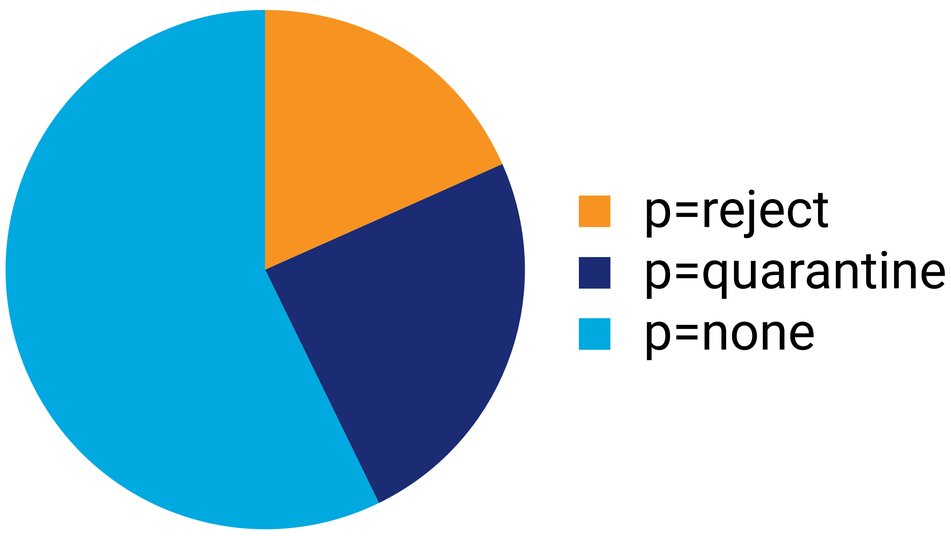


According to our research, only 19.5% of EU IT company domains have a DMARC policy in place, which means they are largely failing to adopt DMARC, thus leaving their domains unprotected.

DMARC adoption in EU IT companies by policy

The following graph shows the proportion of each DMARC policy among EU IT companies by the end of 2021.

EU IT companies DMARC Adoption



Even among EU IT companies that have adopted DMARC, more than half still haven't reached "p=quarantine" and "p=reject" policies.

DMARC Policy mix in November 2021

Prevent fraud and phishing attacks with DMARC today

DMARC is a solution that guarantees the legitimacy of your emails by protecting your brand from fraud and helps to gain visibility and control over your domain.
EasyDMARC focuses on usability, security, reliability, and efficiency. Our team of experts is always ready to assist with your DMARC management and monitoring.
If you want to learn more about DMARC or to adopt this globally-renowned email security protocol, visit our informational blog or send us an email at sales@easydmarc.us.