DMARC Guide for Education IT Staff

"Education and Research still leads as the most targeted industry, with an average of 2,27+ attacks against organizations every week showing a 44% increase compared to 2021."

Check Point Research, *2022 Mid-Year Report*

Email Communication Trends in Education

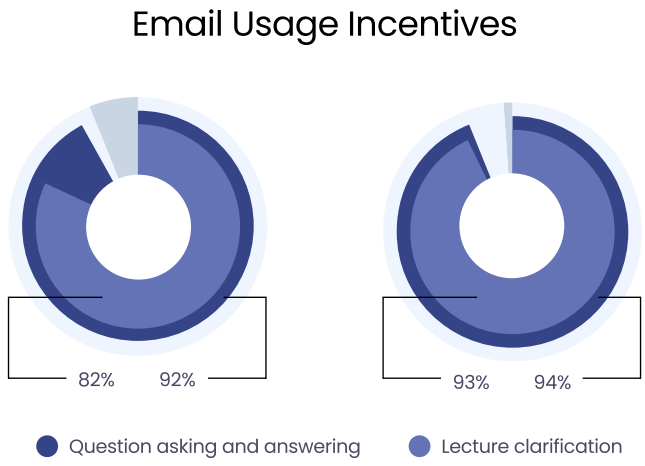
Communication between faculty and students is a crucial attribute in the educational process. It's no surprise, as the precursor to email as a communication method was also developed within the academic context.

MIT's Compatible Time-Sharing System (CTSS) was invented for information exchange among researchers in the 1960s. It allowed multiple users to access a centralized computer network simultaneously via remote terminals. With a "bare bones" command line interface, researchers could also send messages to each other, regardless of location.

Before CTSS, this mode of communication was limited to single-computer users. The system **revolutionized electronic interaction,** paving the way for the widespread use of email as we know it today.

Indeed, email is a universally adopted tool in the education industry. It's cost-effective, allows for easy and accessible information sharing, and promotes quick and efficient communication among students, faculty members, and administrators.

According to one Educause study, faculty (94%) and students (99%) believe email use is appropriate for assignment clarification, question asking and answering (92% and 94%, respectively), and lecture clarification (82% and 93% respectively). 58% of faculty and 66% of students also agree that email usage is **appropriate for relationship building.**



Another study found that email was the primary tool of collaboration for communication among individuals, scientists, and scholars. This isn't surprising, considering student–faculty interaction has been shown to promote and enhance positive outcomes for students (Vol 9, Jalt Call Journal, 2013).

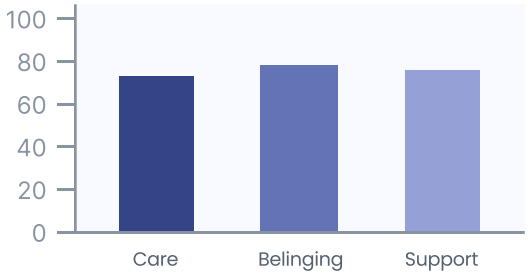
Although digital communication channels like email were already commonplace in the education sector, the COVID-19 pandemic revolutionized distance, synchronous, and asynchronous learning on a grand scale.

Educational institutions became even more reliant on email communication to organize and maintain daily activities, facilitate collaboration, and promote the feeling of unity among various student groups.

The strong correlation between students' educational outcomes and effective faculty communication was brought to the forefront, with electronic mail playing a major role in nurturing that connection.

For example, in Pate AN et al, 2022, almost **80% of students** indicated email response time impacted their **feeling of value** as an individual and whether faculty valued them as a student.

Emotional support during COVID pandemic



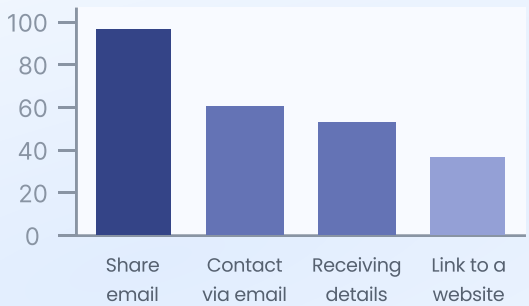
A survey conducted at the height of the pandemic found that 77% of students felt personalized communication made them feel like their institution **cared** about their success; 79% felt a sense of **belonging**, and 75% appreciated **covid-related messages.**

In addition to the daily email exchange between teachers, students, and various departments among educational institutions, the age of email marketing enters the picture.
Email is vital to new student acquisition and shareholder nurturing campaigns among universities, colleges, and learning centers. Below are some statistics highlighting the importance of email in the context of educational marketing efforts.

Email Statistics in Education

According to RNL's 2021 E-Expectations Trend Report, email is the top preferred communication tool for students. 97% are willing to **share their email address**, 53% contact education institutions **via email**, and 51% prefer email responses after **requesting more information**. 42% of students also link directly to a college website from an email.

Preferred Communication Tool for Students



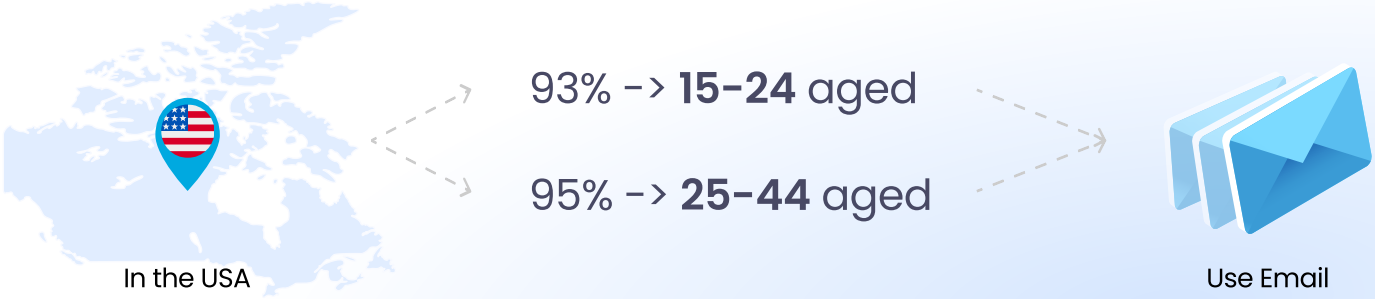
Email also ranked as the third most influential source in students' college searches, tied with videos of campus and classrooms. Despite social media dominance, email **signups increased**, averaging 34.9% weekly in 2020.

When it comes to customer acquisition, email is 40 times more effective than social media. Email is 40 times more effective than Social Media.

Email marketing can help educational institutions boost enrollment, enhance their school brand, and increase student retention rates. It can also yield a substantial return on investment (ROI) with up to $36 for every $1 spent.

Return on Investment: $36 for every $1 spent

According to Campaign Monitor, emails in the education sector have a **higher open rate of 28.5%**, compared to the overall average of 21.5%.
In the US, 93% of people aged 15-24 and 95% aged 25-44 use email.



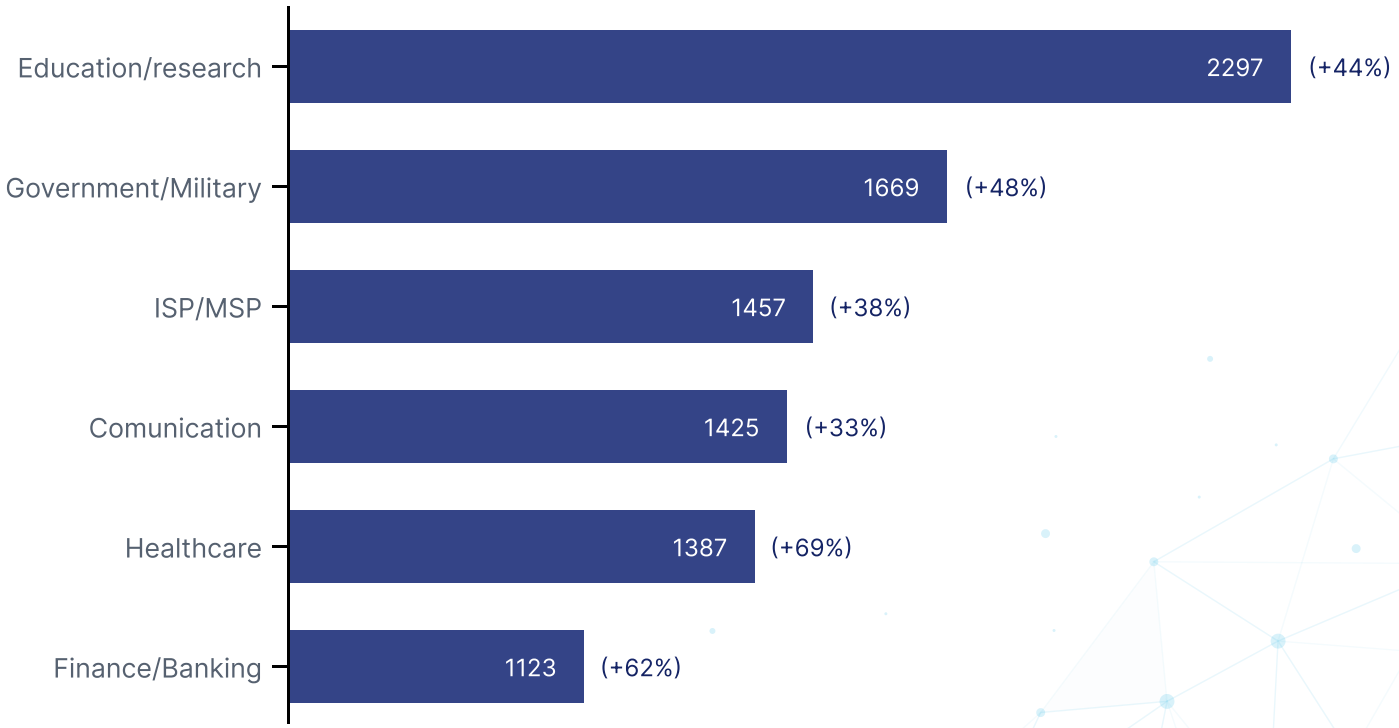
Email Authentication: Why It Is Important for Education Institutions

The above statistics clearly illustrate that outbound email is the livelihood of any educational institution. Thus, maintaining security is of the highest priority.

Educational institutions hold a large amount of **personally identifiable information (PII)**. it takes years to build trust and nurture relationships with stakeholders. Still, even a small security breach could have devastating consequences for an organization's reputation.

In addition to personal information, educational institutions also collect **sensitive financial data**, which is not always well-protected. This makes them a common and lucrative target for cybercriminals.

In the first half of 2022, the education and research sector experienced a **44% increase in cyberattacks globally**. According to Checkpoint's 2022 Cyber Attack Trends Mid-Year Report, an average of 2,297 attacks were leveraged against organizations weekly, making it the most targeted industry for the period.



Percentage increase in cyberattacks in 2022 compared to 2021 (Source: Check Point)

The above report also indicates that email-delivered attacks represented 89% of all "in the wild" cyberattacks. Meanwhile, 61% of all **malware payloads are attached to emails** as malicious "Microsoft document" file types.

A lack of cybersecurity awareness among students, faculty, and administrators are also a major cause for concern. Scholars and employees using unsecured devices to access an already-vulnerable email infrastructure or organizational network give hackers an abundance of easy opportunities to execute targeted attacks.

> All it takes is for one teacher, student, or parent to click on a phishing email created by a cybercriminal and a ransomware attack could be underway.

Omer Dembinsky, Check Point Data Group Manager

In the US alone, 56% of K-12 schools and 64% of higher education institutions experienced ransomware attacks in 2021, according to digital security firm Sophos.

In September 2022, such an attack hit the Los Angeles school district, resulting in an unprecedented shutdown of its computer systems. The FBI later released an advisory, warning that **ransomware attacks are expected to increase in 2023.**

Meanwhile, security firm Barracuda Networks found more than 1,000 educational organizations were targeted by spear phishing attacks in 2020 alone. The researchers also found that educational institutions are more than twice as likely to fall victim to a Business Email Compromise (BEC) attack than the average organization.

Other major incidents noted in the report include the $2.3 million loss experienced by the Manor Independent School District in Texas due to a sophisticated email phishing campaign and the $3.7 million theft from Scott County Schools in Kentucky due to a fraudulent email.

Based on the above facts, **cybersecurity should be the first priority for educational institutions.** Hackers steal valuable data, infect systems with malware, and hold organizations hostage with ransomware - by attacking the tools of communication that institutes use. And usually, email is their first choice.

Why Education Needs DMARC

01 Establishing Infrastructure Visibility

Every security team aims to **have control** over the systems they manage. DMARC lets you know exactly what's happening in your email domain infrastructure.

Whether you're interested in how many emails were sent from your organization's domain, what percent of them were unauthorized, or where your sending sources originate from, **a proper DMARC service provider** will give you the tools to get that information.

02 Maintaining Brand Image and Reputation

It's simple: taking action to prevent impostors from posing as your organization improves brand image. It **increases trust** among email contacts inside and outside your organization while promoting more transparent communication.

By establishing and maintaining robust email authentication standards, students, employees, and stakeholders know that your organization takes cybersecurity seriously.

03 Protecting Stakeholders

If unauthorized emails fail to be delivered, you can be sure that no spoofing or phishing attack can reach a recipient. This **mitigates data theft** and other cyberattacks that could cost your organization dearly.

04 Improving Email Deliverability

Email deliverability is a bit of a side effect of an **increased domain reputation** rather than a direct technical outcome of DMARC implementation. Still, it's what you'll eventually achieve. All of your emails reach the inbox of your intended recipients. No compromises.

Solve the Problem

Let's face it: the IT teams in educational institutions deal with many issues, including **the human factor.** Whether it's maintaining a virus-free environment in the computer labs or ensuring that nobody accidentally clicks the dreaded phishing link, it's a challenge that involves people with various levels of computer literacy and digital hygiene.

> Preventing "cybersecurity fires" is always easier than putting them out.

A proactive IT department considers every possible scenario to avoid undesirable outcomes.
In the case of email security, **the answer** to the issue is email authentication and, specifically – DMARC deployment.

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting & Conformance) instructs receiving servers on how to deal with unauthorized emails from your domain. Simply put, the protocol allows you to determine whether an unauthorized email (purporting to be legitimate) should land in a receiver's inbox, spam folder, or not be accepted at all.

DMARC lets your domain "prove" that authentic messages come from your organization vs. some unsavory character sitting in a garage collecting personal credentials as trophies and selling them to third parties for profit.

The protocol stops malicious actors from impersonating employees or students with fake organizational email addresses while protecting recipients from fraudulent scams.

DMARC Implementation Challenges for Education IT Staff

Security professionals **understand the importance of automated and flexible products** while building infrastructures. IT teams in educational institutions constantly deal with growing technological demands, the human factor, old hardware, and legacy systems. Adding another allegedly challenging task to the team's to-do list might seem unnecessary.

> Still, skipping DMARC could cost you more than the team effort of a few weeks.

Let's see what IT teams need for successful DMARC implementation.

DMARC Takes Leadership

Everything begins with **a decision:** "Our organization needs DMARC." Someone has to take responsibility for reaching the DMARC "*reject*" policy and hold the whole team accountable throughout the enforcement journey.

DMARC Takes Teamwork

However, one person isn't enough. The whole security **team needs to be in** on the project, as DMARC deployment is a meticulous process. Source identification and configuration require a cross-team effort.

DMARC Takes Time

There's no overnight success in DMARC implementation. Depending on the size of your organization and email sending volumes, your journey might last anywhere from a couple of weeks to several months.

DMARC Takes Maintenance

Your domain needs **continuous DMARC maintenance.** Not following through can bring even more devastating results. Setting up the record in your DNS might create an illusion of being protected while bad actors are still lurking in your domain environment.

DMARC desertion is a common practice among security teams. Even if you've finally reached the "*reject*" policy, periodical maintenance of your domain infrastructure, including sending source reviews and record updates, should be on your to-do list.

> Reaching DMARC compliance is challenging, so you need a reliable and integrated cloud DMARC solution to improve your experience.

DMARC Adoption Throughout Educational Institutions

EasyDMARC researched a total of 1,930 .edu domains in the US, and found that only 152 have reached the "reject" policy. In other words, only **7.8%** of the sample is fully protected against spoofing and phishing attacks. While this statistic is alarming, it's still better than the situation worldwide.

Our research shows that out of 12,050 randomized .edu domains, only 401 have reached "*reject*," which translates to a **mere 3.3%.**

In addition to the domains that use the *p=reject* policy, we've classified the samples of US-based and worldwide domains using the following criteria:

Classification criteria	US Total of 1930 .edu domains	Worldwide Total of 12050 .edu domains
DMARC record exists for the domain	58.1%	20%
P=none	43.9%	14.1%
P=quarantine	10.3%	3.9%
DMARC record doesn't contain "mailto:"	3%	2%
SPF record exists	93.8%	45.6%
Reject	7.8%	3.3%

In the US-based .edu sample, the number of domains with a DMARC record is 1,122 (58.13%). However, **filling in the empty slot** for the DMARC record won't protect your email infrastructure. It's just the beginning of a process that leads to DMARC policy advancement.

Most interesting is that almost 94% of the total researched domains have successfully deployed **the first step of email authentication** – they have an active SPF record. Still, let's not forget DMARC works based on SPF and DKIM protocols.

> Setting up SPF is only one-third of the email authentication journey. Going all the way is the difference between fully protected infrastructure and half measures.

In our sample, **848**. edu domains have set their DMARC to "monitoring mode" (*p=none*), while only **199** worked on advancing it to *p=quarantine*. This leaves the door wide open to malicious actors and costly cyberattacks.

Want to simplify DMARC implementation and monitoring for your **.edu domain?**

Contact Us

Take Domain Protection to a New Level with EasyDMARC

We've already agreed that DMARC deployment is **challenging and meticulous**, but it doesn't have to be. EasyDMARC is here to save you time and effort. Here's how.

Managed Services

Tackle all your DMARC-related tasks in a human-friendly workspace

Your **EasyDMARC dashboard contains all the answers** – everything from DMARC record updates to report management and source alignment is available in a non-technical, easy-to-understand, and interactive platform.

Cloud Native DMARC

Stay flexible during DMARC setup – no need for legacy applications

Access your EasyDMARC dashboard from anywhere, save your progress, and return whenever and wherever you choose to take the next step in email authentication.

EasyDMARC = Peace of Mind

Stay on top of DMARC-related issues with alerts and weekly reports

Large domain infrastructures might overwhelm even the most seasoned professionals. **EasyDMARC's automated platform** follows all DMARC events and sends smart notifications. You'll always know what's happening in your email ecosystem and you'll never have to worry about missed issues.

Other AI-Powered Features

Meet your domain management needs with smart solutions

Whether you want to check your domain reputation, see if a text contains suspicious URLs, or test email issues, **our AI-powered solutions** make it a quick, easy, and seamless process.

> DMARC might be challenging, but your peace of mind is worth it.

How EasyDMARC Helped Newman University

Newman University is a college based in Kansas, US. It has a large urban campus, around 4,000 students, and a graduation rate of 70%. Student and faculty security, email deliverability, and DMARC reporting should be the highest priority for an educational institution of this size.

Before coming to EasyDMARC with their issue, Icer Vaughan, Newman's Chief Information Officer, had already tried implementing DMARC at the university. However, without managed services, an easy-to-use dashboard, and smart email domain management, the university gave up very soon after they started implementation.

When Newman university reached out to EasyDMARC at the recommendation of one of the university vendors, we knew exactly what they needed.

> Excellence in the product, risk-free deployment, reliable support through onboarding, and full domain infrastructure visibility is what EasyDMARC is good at.

By choosing EasyDMARC as your DMARC vendor, you buy clarity and confidence that your organization's **brand image will be protected from impostors** swiftly and successfully.

Start Your DMARC Journey