EINPRESSWIRE

DMARC and Educational Institutions in the USA

MIDDLETOWN, DELAWARE, THE USA, September 15, 2022 / EINPresswire.com/ -- Amid and post the worldwide pandemic, most industries have relied primarily on digital, and educational institutions in the USA are no exception. However, as much as these institutions are enjoying the benefits of online operations, they're jeopardizing the security of students, staff, and other stakeholders. They exchange unsecured emails for communication, and hackers know how to exploit such security vulnerabilities.

Per a public service announcement issued by the FBI, threat actors have found ways to use institutions' email domains to send fraudulent emails to students with a promise of employment. The emails contain information about fictitious positions, and victims are tricked into purchasing software before they start the "job." The software may or may not contain malware, but those who fall for the trick, lose money.

This is only one example of how bad actors leverage university email addresses. However, there are ways to keep the domains free of such phishing and spoofing attacks. Enter EasyDMARC's expert team with their research about email security practices of educational institutions in the USA. Keep reading till the end to learn everything about what they found.

But before that, let's briefly discuss the US education system.

Education Institutions and Stages in the USA
Education in the USA is offered through private schools, public schools, and homeschooling. The overall standards are set and supervised by the state government. Compulsory education consists of three levels: elementary, middle (junior) school, and high school.

Elementary school, also called primary school, is the first seven to nine years of formal education. Middle or junior schools are varying combinations of grade fifth to grade ninth. In this stage, students get more independence and study subjects like math, social studies, science, English language, arts, and sometimes other foreign languages. High school is the final stage of secondary education in the USA, most of which include grades ninth to twelfth. Typically, high school students fall under the age range of 14 to 19 years.

Secondary education includes people with a high-school diploma going to colleges and universities for a specialization. To receive a bachelor's degree (BA), an individual must go through four university years. As an option, students can spend their first two years at a community college and then transfer to a four-year college. Individuals who don't want a BA can complete an associate degree, which they can acquire in two years.

Graduate school allows for a master's or a doctoral degree. It advances the students into the field of study and usually includes research or fieldwork of some sort.

What is DMARC?
Everyone's obsessed with cybersecurity these days. However, in most cases, it doesn't show. There are a few reasons for this, but the heftiest one is that cybersecurity is hard to achieve. While everyone uses email as a communication method, it remains one of the most neglected areas of cybersecurity. DMARC spooks many business decision-makers. But let's diffuse your fears.

DMARC, or Domain-Based Message Authentication, Reporting, and Conformance, is an email authentication protocol that uses SPF and DKIM to evaluate the authenticity of emails sent from your domain.

SPF or Sender Policy Framework enlists all hostnames and IP addresses permitted to send emails using a specific domain. Senders outside of that list are recognized as inauthentic. DKIM or DomainKeys Identified Mail uses digital signature encryption for email authentication. An encrypted signature goes to the recipient's server along with an email to verify its authenticity.

Since DMARC is based on SPF and DKIM results, at least one of them has to be in place. You need to publish a DMARC record in the DNS to direct recipients' servers to how to treat your emails as per the policies.

DMARC has three policies:

None policy (p=none): It enables the receiver's mailbox to do nothing with unqualified emails. However, they're added to the DMARC record for any infractions.
Quarantine policy (p=quarintine): It sends unsolicited emails to the spam folder.
Reject policy (p=reject): It tells the receiver's mailbox to welcome only 100% verified emails and

denies the entry of all unqualified ones.

Why is DMARC Important for Education Institutions?

Since educational institutions hold tons of sensitive data of students and staff (like contact details, residential addresses, medical reports/ history, mark sheets, financial details, etc.), they become highly attractive to cyberactors.

Moreover, the pandemic has propelled us to shift rapidly to digitization, increasing the cybersecurity challenges for this industry. The email has become the primary communication medium between students, teachers, parents, and other stakeholders.

With adaptation to remote and hybrid learning, the number of email-based cyberattacks on educational institutions in the USA will continue to soar. Unprotected email domains are common across the education sector, jeopardizing several parties to hoaxed email messages sent in your institution's name.

DMARC Adoption Among US Colleges and Universities

EasyDMARC's marketing team conducted a survey and found that out of 252 educational institutions in the USA, only 133 have deployed the DMARC policy, which translates to just 52.77%. The number of institutions using none, quarantine, and reject policies are 88, 19, and 26, respectively.

Basically, only 26 out of the researched 252 colleges and universities are fully protected against phishing and spoofing attacks.

However, it's positive to find that 224 out of 252 (88.88%) educational institutions have SPF protocol in place.

How to Add DMARC to Your DNS?

If you decide to embark on your DMARC journey, you need to know how to add DMARC to your DNS provider. EasyDMARC offers a free DMARC Record Generator Service that guides you through each step.

Summary

Hackers target educational institutions to attempt email-related cyberattacks as they hold sensitive details of students and staff. They often try phishing, spamming, and spoofing tactics using the email domain so that the recipients perceive it to be coming from a trusted source. This convinces them to take action.

A cyberattack not only fools the recipients but also damages your institution's reputation. Thus educational institutions must deploy SPF, DKIM, and DMARC authentication protocols.

Anush Yolyan
EasyDMARC Inc.
+1 8885635277
email us here