

/LIBRAESVA

Avoiding email attacks in 2023

A PRACTICAL CHECKLIST FOR
EDUCATION NETWORK MANAGERS



ENTER NOW →

/ CONTENTS

03

Why the education sector needs email security

04

Threats in the education sector today

05

Email. The ideal 'attack vector'

07

Stopping a Business Email Compromise Attack.

09

Check List for avoiding a data breach in 2023

12

See For Yourself the Gaps in your Defences

14

Why Libraesva?

/WHY THE EDUCATION SECTOR NEEDS BETTER EMAIL SECURITY

THE EDUCATION SECTOR RELIES ON EMAIL

Schools, colleges and universities all rely on email to function. It's the primary method of communication between staff, students, the school and parents. Families able to fund private education are seen as high-value victims by fraudsters.

SAFE GUARDING IS A PRIORITY

Most schools agree that embracing technology and digital strategies improve learning and pupil development. However, in adopting digital systems like email, students are opened up to the receipt of content from the outside world. It is essential that students have a safe learning environment and that emails sent to them do not contain inappropriate or illicit content, such as drugs, violence, bullying, radicalisation or even adult images.

EXISTING DEFENCES ARE OFTEN INADEQUATE

Schools often trust their email service provider or Microsoft to secure email. Unfortunately, inbuilt security provisions are often inadequate, which can lead to staff or students unwittingly opening and interacting with email attacks.

CYBER-ATTACKS ARE INCREASING IN SOPHISTICATION

While simple cyber-attacks still very much exist, ever-more sophisticated attempts are now increasingly common. For example, after successfully compromising a school's email system, cybercriminals are able to launch further attacks on partner schools and organisations. By leveraging the trust built up by existing relationships, not only are the other schools and businesses adversely affected, but crucially so too is the 'host' school's hard-won good reputation.

PREVENTION IS BETTER THAN CURE

The costs of a successful cyber-attack soon add up. There are the obvious costs, such as those associated with service disruption, and the costs of restoring compromised systems. There are also support costs, in which staff must respond to stakeholder concerns. And let's not forget legal costs and financial penalties, which often dwarf all other costs combined.

PEOPLE MAKE MISTAKES

Errors made by members of the faculty & staff, are responsible for more than 90% of all major data breaches. 90% of all cyber-attacks originate from an email. It is imperative then to ensure adequate email security layers are in place, to significantly reduce the threat of attackers reaching users' inboxes.

/THREATS IN THE EDUCATION SECTOR TODAY

SCHOOLS

85%

OF SCHOOLS REPORT RECEIVING PHISHING ATTACKS

31%

OF SCHOOLS REPORT RECEIVING MESSAGES FROM CRIMINALS IMPERSONATING OTHERS

13%

OF SCHOOLS REPORT RECEIVING MALWARE ATTACKS

COLLEGES

91%

OF COLLEGES REPORT RECEIVING PHISHING ATTACKS

58%

OF COLLEGES REPORT RECEIVING MESSAGES FROM CRIMINALS IMPERSONATING OTHERS

30%

OF COLLEGES REPORT RECEIVING MALWARE ATTACKS

UNIVERSITIES

86%

OF UNIVERSITIES REPORT RECEIVING PHISHING ATTACKS

75%

OF UNIVERSITIES REPORT RECEIVING MESSAGES FROM CRIMINALS IMPERSONATING OTHERS

39%

OF UNIVERSITIES REPORT RECEIVING MALWARE ATTACKS

Source: UK government Cyber Security Breaches Survey 2021

/EMAIL.THE IDEAL 'ATTACK VECTOR'

WHY CYBER CRIMINALS LOVE EMAIL

Email is the primary communication tool across education today. It conveniently stores our internal conversations, our important discussions with partners and crucially, confidential communications between staff and students. What's more, it can house data relating to **HR matters** and **documents from other critical business functions** such as our financial and legal departments.

Access to almost every service we consume from banking to utilities, social media and other business-related platforms can all be recovered by email. A compromised email account therefore, could be the key to accessing everything else.

EMAIL. THE IDEAL 'ATTACK VECTOR'

Email's widespread uptake allows cybercriminals to target almost anyone, from anywhere, providing them with a wide range of means and vectors to deliver attacks. Such as using **URL links** to redirect users to **malicious websites** containing malware or by exploiting common document types such as **Microsoft Excel, Word** and even **PDF's**. The hosting of malware in services provided by **Dropbox, Google Docs** and **Microsoft OneDrive** is also on the rise.

Social engineering is also used in an attempt to deceive individuals into revealing sensitive information. Cybercriminals often impersonate schools and other institutions, leveraging the reputation and trust that exists between them and their partners.



With cybercriminals leveraging their relationships to **steal information and/or extort funds**.

From the perspective of a cybercriminal then, email is **the ideal 'attack vector'**. Indeed, FBI research shows losses from Business Email Compromise and Email Account Compromise cost **\$2.4bn* in 2021 alone**.

/EMAIL.THE IDEAL 'ATTACK VECTOR'

WHY YOU NEED TO KEEP ON TOP OF YOUR EXISTING DEFENCES

Many schools are still heavily reliant on **Microsoft** and **Google's "built-in" email security features** or on the basic controls offered by email clients. Unfortunately, these platforms often lay the onus firmly on the end-user to keep security policies and configurations up to date, leaving over-stretched staff to do their best to spot and prevent attacks.

This is incredibly difficult to sustain without a well-resourced and well-funded **IT facility**, which is a luxury many educational institutions do not have. IT staff are often overloaded, meaning security can often be neglected. In many cases security tools are never fully deployed to their maximum effect.

CLOSING THE SECURITY GAP IS POSSIBLE.

The good news is it is possible to close this gap with a little help from your friends. A specialist email security vendor with a full understanding of the security landscape can ensure you have **the most up to date security capabilities in place at all times**. Proactively developing and innovating as the landscape evolves is one of the biggest benefits of partnering with a best in breed email security provider, whose business is **100% focused** on the specific area you are employing the technology to secure - email.

However, **no single solution is 100% effective** and the level of protection required from one institution or school to another can vary greatly and can depend on many factors.

SOLVING THE PROBLEM IN A FEW SIMPLE STEPS

For the most effective defence against cyber-attacks from email, **a combination of tactics is sensible**. Deploying an innovative email security solution in isolation is not enough. This needs to be augmented with the **extensive training of users** within your school or establishment, to **highlight the potential dangers posed by cybercriminals**, to increase awareness of their methods and ultimately to mitigate against the risk of a data breach.

/STOPPING A BUSINESS EMAIL COMPROMISE ATTACK.

THE WOLF IN SHEEP'S CLOTHING.

SPOTTING A BUSINESS EMAIL COMPROMISE ATTACK.

"IN 2021, THE FBI RECEIVED 19,954 BUSINESS EMAIL COMPROMISE (BEC)/ EMAIL ACCOUNT COMPROMISE (EAC) COMPLAINTS WITH ADJUSTED LOSSES AT NEARLY \$2.4 BILLION."*

**FBI IC3 REPORT 2021*

Email security technologies are available in several flavours but ultimately all of these solutions aim to keep the volume of spam emails to a minimum and to detect dangerous content, malicious links and files and documents from being delivered to users' mailboxes.

Many of these technologies look for the most common traits of a malicious email, including blacklisted IP addresses or a dodgy domain.

Quarantining the emails and then keeping them well away from the recipient.

But what happens when the email is coming from a trusted source? From a legitimate but compromised partner school or institution that you may have even whitelisted, where you know and trust the organisation and the individuals within it?

Simple Mail Transfer Protocol (or SMTP) wasn't originally designed with security in mind. This has meant email, without the right protection, can be wide open to potential data theft using a simple, yet effective attack, with someone else using your domain to target others.

It's simple, even for those with a limited understanding of coding, for someone to be able to impersonate a user. A short google search easily yields a step-by-step guide to launching an **email account compromise attack**.

The intended target could be **stephen.reynolds@libraesva.co.uk** but the cybercriminals have bought a similar domain **stephen.reynolds@libreasva.co.uk**. To the naked eye, you may not recognise the difference at first glance, but the domain is live and fully under the cyber criminal's control.

Without the right measures in place, the fraudulent email the attacker then sends to the finance department of Stephen's organisation, requesting payment, would be delivered unquestioned.

/STOPPING A BUSINESS EMAIL COMPROMISE ATTACK.

STOPPING A BUSINESS EMAIL COMPROMISE ATTACK.

It's vital that you conduct regular phishing simulation and testing on your business users to monitor and understand their behaviour and to improve their ability to detect and report dangerous emails and phishing attempts. Users that fail these test campaigns can be provided with additional training to prevent a real cyber-attack from being successful. **Training is best delivered in short videos to correct behaviour and provide bite sized information that is easily digested.**

Staff and students are generally not trained cyber security professionals, so security defences should be in place as a minimum to block and prevent the bulk of unwanted or dangerous emails from reaching your users. **Leaving just a small % of ambiguous cases for IT staff to have to deal with on a weekly or monthly basis.**



/A PRACTICAL CHECK LIST FOR AVOIDING A DATA BREACH IN 2023

We have compiled a check list of capabilities that we recommend you should have in place, as a minimum, to provide you with the greatest chance of mitigating email borne cyber threats causing a data breach to your organisation.

SECURE ACCESS

The first step to securing email is controlling access for your users to your email infrastructure. **Multi-factor Authentication** provides a method of secure access to the system, using 2 different forms of authentication to prevent unauthorised access to the system. Which would prevent access even in a situation where the password has been compromised.

It's also important to reject any emails from external senders to invalid users to avoid any unwanted threats from being stored in your mailboxes. The email defences should securely connect and dynamically synchronise with the email service you are using. Ensuring user creation is automated and recipients are validated or removed if they are no longer current.

INBOUND

Your email defences **should contain a multi-layered approach** to the scanning of inbound emails. Analysing the header and the body of the email. Thoroughly scanning attachments and links and providing protection against all forms of phishing and social engineering attacks.

It should include the ability to remediate emails from your users' mailboxes. Such as where the email wasn't meant for that individual or for threats missed by your defences that are later identified, so you can safely remove the email from users' mailboxes.

SPAM FILTERING

Advanced anti-spam filters combine a range of different checks to analyse the SMTP related information of the email header and the body of the email itself. Performing checks on the sender's IP and network related information and the reputation of the sending mail server against a number of private public sources. They should also prevent marketing **emails (graymail)** where users may have signed up to a service and began receiving emails they were not necessarily wanting.

ADVANCED ATTACHMENT FILTERS

Capabilities to detect all malicious file types and file extensions are essential to avoid users receiving executable, **Script Python** and **Batch** files. There are 50+ malicious file extensions in the wild. Attackers package the harmful programs into file types such as **ISO images, ZIP** and **RAR formats** that provide a convenient way to disguise the program's intent. Coverage should also be extended to **Media files (MIME types)** such as **Elf, Registry, Installer, Self-extract**.

/A PRACTICAL CHECK LIST FOR AVOIDING A DATA BREACH IN 2023



MALWARE & RANSOMWARE PROTECTION

Emails should be vetted against a comprehensive set of threat detection engines. Using multiple antivirus engines for known signature-based detection and heuristical and behavioural analysis.



ADVANCED FILE SANDBOXING

Due to the evolution of evasion techniques, the **absence of time for analysis in an email setting and the complexity of traditional virtual machine-based sandboxes**, the **"traditional"** approach of detonating files and monitoring behaviour has proved ineffective.

Your defences should only permit files that are performing **"safe"** operations for that document type. If the document is performing any operations, **not in the "safe list"**, such as accessing the file system, deletion or calling down third party applications from the internet, the sandbox should be able to sanitise and remove the **"active contents"** or the dropper from the attachment and disarm the file. Delivering the sanitised version to the user and isolating the original in quarantine. Should the attackers manage to crash the sandbox or create a technical disruption to the analysis, a fall-back action should exist to block the entire document. As part of the detection, the sandbox should also be able to detect the presence of the evasive indicators and block the file should any obfuscation or evasion techniques be present.



ADVANCE URL SANDBOXING

Your email defences should have capabilities to re-write links within emails that provide **"time of click protection"**. The URL sandboxing technology should dynamically scan the website and any redirects to detect suspicious behaviour, malicious content such as **javascript** and **other embedded objects or code**. Users should be prevented from accessing the site if any of these are found, only allowing users through if the site is clean.



SAFEGUARDING PROTECTION

Your defences should have the ability to scan the body copy of emails for keywords that you are prohibiting, to prevent them reaching students and to provide a safe learning environment. Safeguarding content may include: **Illicit drugs, abuse, violence, radicalisation, grooming, bullying** and **digital currencies**.



/A PRACTICAL CHECK LIST FOR AVOIDING A DATA BREACH IN 2023

✓ OUTBOUND

The same security analysis provided for inbound email should be extended to outbound email traffic. This is to ensure that your own employees are not able to send out malicious content to external recipients. Some email security solutions automatically exempt the email from any further checks if a **domain** or **IP address** is whitelisted. You should ensure that this is not the case as this **creates a serious security risk to your organisation** when emails are coming from these trusted sources.

The ability to retract emails sent to individuals that users have not previously spoken with, is highly desirable. **This prevents emails from being sent to the wrong contacts and an added step for data loss.** The message can be recalled by the user, within a short hold period, before its release if not actioned so emails are never held and forgotten about indefinitely. This capability should not be included for every email.

✓ END TO END ENCRYPTION

Transport layer security (TLS) should be enforced as standard to encrypt the communication tunnel between your email server and the intended recipients. This prevents interception of the traffic in transit. Further capabilities to ensure confidential information is sent fully encrypted and can only be read by the intended recipient of the email. This will prevent the content from being stored in plain text in the recipient's mailbox, due to the nature of the content that should be protected, even if the recipient's mailbox has been compromised.

Some security providers opt to store your encrypted emails on an encryption server and require the recipient to register and authenticate. Exposing your users to this approach can increase the chances that a fraudulent phishing campaign, with a look-a-like landing page, may trick your user into submitting their details as they are familiar with the process. For maximum security and to remove the need for recipient registration, **an encryption key should be delivered to the sender** of the encrypted message and the key provided to the recipient by any other means other than email. For data protection, all **your encrypted emails should be stored on your email security system** and not on shared cloud infrastructure.

✓ DATA LOSS PREVENTION

Ensuring sensitive and confidential information is not leaked externally is critical. Your email defences should contain a way to analyse and detect emails for patterns in the subject and the body. Types of contents may include **Credit Card Numbers, Social Security Numbers**, wild card 16 digit keys or 8 digit passwords. They may even include **Engineering blueprint numbers** that have 3 letters followed by 4 numbers. The type of content may vary and be unique to your organisation and policies. Flexibility of rules to perform different actions based on the content found should be available to not only block or prevent the email from being sent but also forward the email to a shared mailbox to monitor **DLP infringements** with the ability to score the content based on its severity and desired outcome.

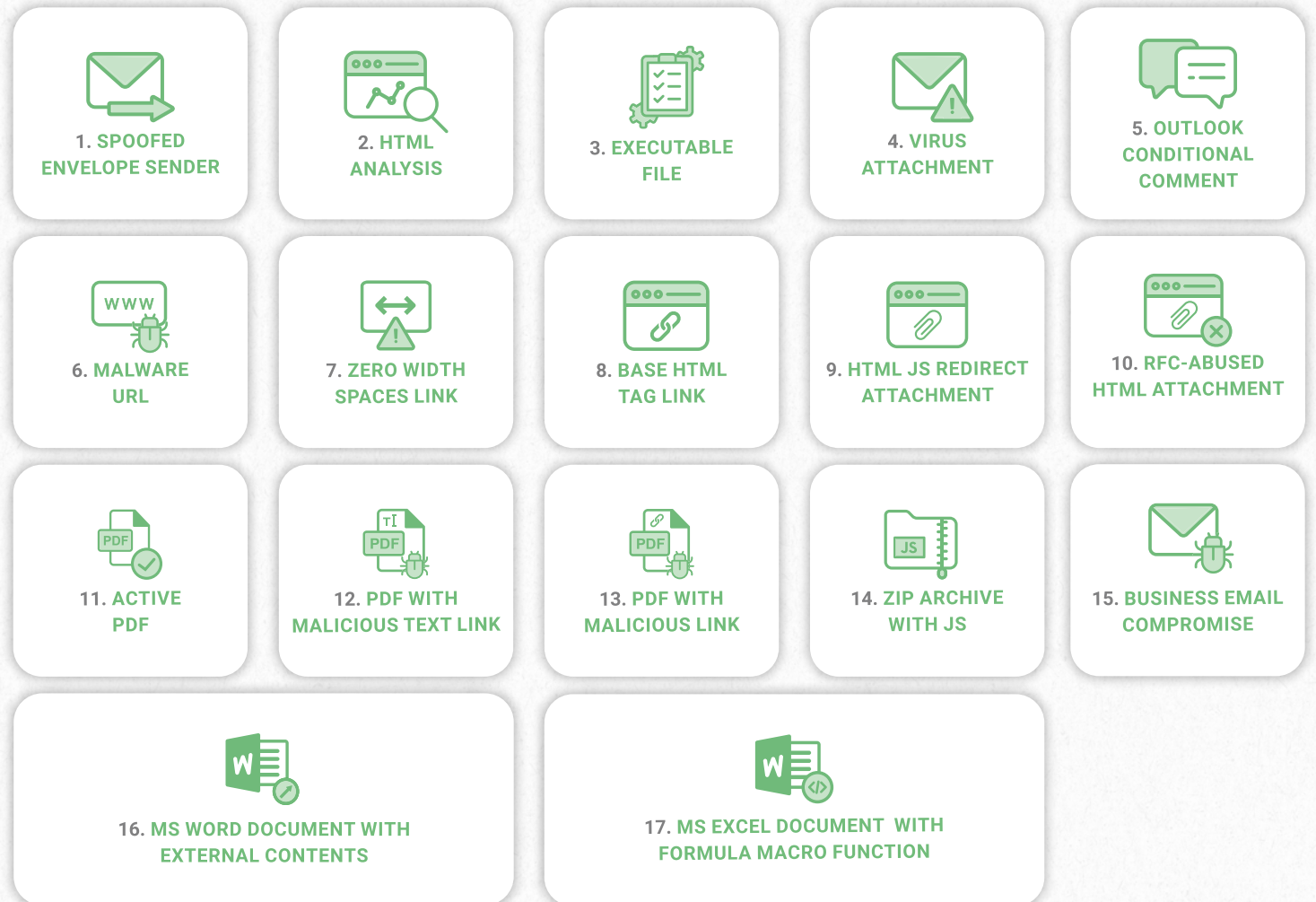
/SEE FOR YOURSELF AND UNDERSTAND THE HOLES AND GAPS IN YOUR DEFENCES

Regardless of whether you have measures in place or are considering implementing a robust email security solution, it is crucial that you test your current security capabilities against the range of potential threats that your business may face.

The Libraesva Email Security Tester Tool

simulates 17 different types of attacks, is simple and takes just 15 seconds.

www.emailsecuritytester.com



/SEE FOR YOURSELF AND UNDERSTAND THE HOLES AND GAPS IN YOUR DEFENCES

The test itself is completely safe and the threats delivered have been disarmed and **will not** cause any damage to your systems. The threats do however behave maliciously and should be blocked by your email defences before they get to the users.

The test is **completely private, non-intrusive** and **requires no setup**. You simply add in the email address that you'd like to run the test on. There is a secondary option to add a **Whaling contact**. This allows you to simulate whether you can successfully stop a business email compromise attack. The Whaling individual's email address you supply here will not receive any notifications or alerts, but we will try to deliver an email that looks like it came from that person to the primary contact.

Once you click go, a confirmation email is sent to you that you will need to confirm to begin the test. Some security vendors block the confirmation email. Which is the first false positive as it's just a clean email with a link to a website. Microsoft may also quarantine the message or move it to junk folder. Simply release it and click **"deliver emails"** to activate the test.



Try it yourself today – www.emailsecuritytester.com



/WHY LIBRAESVA?

HOW DID YOU SCORE, WERE THE RESULTS WHAT YOU EXPECTED?

COMPLETED THE EMAIL SECURITY TESTER TOOL? SCARY ISN'T IT?

Hopefully this has helped provide valuable insight into your current level of protection and that you are now aware of any holes and gaps in your current defences.

ARE YOU THINKING ABOUT ADDING AN ADDITIONAL LAYER OF SECURITY TO YOUR EMAIL?

Selecting an email security vendor can be difficult, so we thought we would share with you why other schools and educational institutions have chosen Libraesva to protect their email.

WE UNDERSTAND EMAIL

We've been working in the field of email **since 1996** and this is our sole area of expertise and our core business. Cyber threats evolve quickly and staying one step-ahead is our focus.

WE UNDERSTAND EDUCATION

We protect **160+ schools and multi-academy trusts**. Our platform has been designed specifically for educational institutions to provide a secure, cloud based solution that's simple to configure and use.



/WHY LIBRAESVA?

WE ARE BURSAR FRIENDLY

We provide an all-in-one licence to our enterprise grade platform. As we develop new features, they are made available to you immediately. There are no costs for technical support or installation services and our engineers will walk you through the entire setup.

TRY FOR FREE

A short 30-day trial of our solution provides you with a risk assessment report that delivers tangible evidence to help justify your investment and to build your business case.

CONTACT US TODAY

 www.libraesva.com/free-trial



/LIBRAESVA


ABOUT LIBRAESVA

Libraesva secures email communications for organisations, helping them **eliminate email borne threats**, **preserve email data** and provide an environment for their people to communicate safely.

With an integrated suite of security, continuity and compliance solutions, Libraesva is **100% focussed** on the needs of mid-sized organisations, where there is an immediate need for simple to manage, **all-inclusive email security** due to the rapidly growing volume and sophistication of threats, complexity of existing security technology, and increasing regulation.

Libraesva has won many awards, has consistently been **certified by Virus Bulletin** as one of the best email security systems, and is trusted by leading brands around the world.

CONTACT US:

 www.libraesva.com

 info@libraesva.com