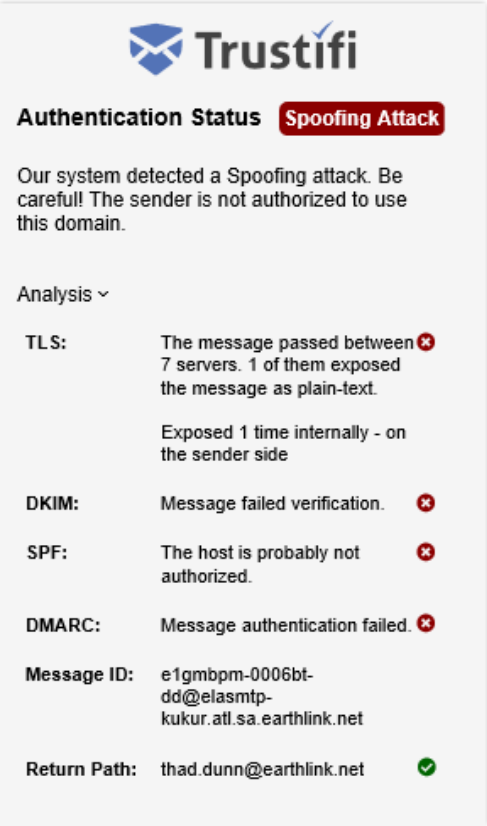
Get email encryption now through the ISBA

Email privacy is crucial to a law firm, but few take email security seriously. Only 36 percent[1] of all attorneys and only 25 percent[2] of sole practitioners use email encryption. Yet, it is one of the easiest steps lawyers can take to help protect themselves against cybercriminal activity.

Not using email encryption in the past was understandable because it was clunky and difficult to use. But this excuse is no longer true or acceptable. Attorney emails have become more and more attractive to cybercriminals. If you haven't been attacked yet, you will be. Verizon's 2018 Data Breach Investigation reports 90 percent of breaches occur via email using phishing or social engineering techniques.



Email encryption is no longer a fringe technology only used by self-professed technology geeks. It is a technology that every firm needs to implement. As your partner in practice, the ISBA wants to help you protect your email. We have spent the past 18 months reviewing a variety of services and ultimately partnered with Trustifi Email Encryption.

Trustifi was selected because it provides an easy to use interface for both the users and recipients. An additional feature is Trustifi's Incoming Email Authentication. This service scans every incoming email and runs a variety of tests to confirm whether the email sender can be authenticated or not. Trustifi provides you an analysis of every incoming email similar to the example on the left. This service is not a replacement for your antivirus programs, rather it is a supplement in identifying phishing attempts and emails with malicious intent.

The ISBA is committed to increasing the use of email encryption by Iowa attorneys and made this service available for $25 annually per email address. If you are interested in protecting your data, please visit http://www.iowabar.org/trustifi for more information.

Here are a few additional tips to help avoid phishing attacks:

- **Educate, Educate, Educate**
- **Be vigilant -** Carefully examine the senders of unexpected or suspicious communications. Often these phishing attempts change only one number or letter within the address. There are many things you can look for that indicate a potential scam:
    - Poorly written or impersonable messages; Look for typos.
    - Messages requesting financial information should automatically be scrutinized.
    - Emails referencing activities (such as orders, shipment notifications, etc.) that you don't recognize.
    - Verify the validity of any wire transfer with a phone call.
- **Carefully verify links provided in emails -** Don't click on the link(s) in unsolicited emails. Even if you recognize the sender, hover over links and double check if the destination URL is what it's

[1] 2017 ABA Techreport
[2] 2017 ABA Techreport

claiming to be. If you wish to be extra careful you should type out URLs manually and avoid links altogether.

- **Research online**: When concerned, do an online search for the email address or content of the email to further investigate the validity of the communication. Often, you can find results showing key components of the email identifying it as a scam.