WHITEPAPER **2020**

Email Security for Legal

www.**trustifi**.com

Trustifi

Cybersecurity is often an afterthought when it comes to firms. Many lawyers and attorneys often believe that hackers would not think of targeting their law firm, and that is an incorrect assumption. About 83% of law firms experienced phishing attacks in 2018.

Lawyer-client relationships are built on trust. If a firm loses a client's trust, then it will lose their business. Many clients require confidentiality and they will not hesitate to ditch a practice if there is a data breach. Law firms range in size from a single attorney to thousands of attorneys. All law firms in unison face the same fight against hackers.

Your client's confidential information could be easily leaked if you are not careful. Patent lawyers deal with confidential information and intellectual property everyday. Hackers are targeting lawyers and attorneys with access to key information as well as financial information. Many law firms have mistakenly sent payments to hackers that posed as vendors.

Even worse is a hacker that is pretending to be a fellow law professional. In 2016, the New York Attorney General's Office noted that several lawyers received emails from hackers that were pretending to be from the office. This trend is only actively increasing.

Impersonating a Lawyer

When working in the law industry it is common to receive confidential and encrypted messages during the workday. Hackers are just starting to catch onto this and they are beginning to impersonate lawyers from various law firms all over the country. They create elaborate emails that would fool even the most seasoned lawyers.

> *How can law firms hope to fend off hackers that are posing as lawyers from legitimate law firms?*

Thankfully, Trustifi has developed an AI powered email security system to help your employees determine friend from foe. The anti-phishing solution is anchored by two separate systems

The first puts the power in the hands of your employees, by utilizing a visual rating system to help users determine who can be trusted and who is a potential threat. When an email is received, Trustifi will scan every part of the email to ascertain if the sender is who they say they are. If any indication of a bad actor is found, Trustifi will warn the user with a bold, colored banner that will describe the type of threat that was found – "Spoofing Attack", "Impersonation Attack", and others. Trustifi will also check if the email contains any malicious links or attachments that may cause harm to those who click on them.

The second piece to this phishing prevention system is an inbound email protection solution that works behind the scenes. Each law firm can create customized rules for how to handle different threats, as lawyers specializing in different areas will require different rules. The system will scan all incoming emails and search for any indications of malicious activity. A suspicious email will be banished from a user's inbox and quarantined, completely mitigating the risk of an employee falling for a hacker's attack is completely mitigated. These two systems will help keep your law firm free from phishing attacks.

Ensuring that confidential documents are not stolen by the opposition or hackers is another concern for firms. If your case strategy is obtained by the firm you are up against, then your entire case could be compromised.

Protect Your Case Strategy With Encryption

Many law firms will stop at nothing to win a case; this includes stealing key documents that a case is based on. Your employees need to encrypt all emails with sensitive data and attachments. However, even the most disciplined employees will forget every now and then to appropriately encrypt an email, It's simply human nature.

Trustifi completely eliminates that problem with an AI powered data loss prevention system that scans all outgoing emails. The system checks both the email's message and the attachments and looks for any content that may be sensitive, including scanned images which are checked using advanced OCR technology. When potentially sensitive content is found, Trustifi automatically encrypts the email and notifies
the administrators so that the user who forgot to encrypt the email could receive additional cybersecurity training. The email sender does not have to take any action, Trustifi's intelligent software takes care of everything for them.

Trustifi also checks for sensitive information being typed in while the email is being composed. When the system finds sensitive information, users will be prompted with a few encryption options that they can choose from. A multi-factor authentication system also keeps your email in the hands of the intended parties only. Trustifi's complete email security solution will keep your law firm secure.

Trustifi also checks for sensitive information being typed in while the email is being composed.

256-Bit AES Encryption

NSA grade protection over your data and files

Extra Security Features

- One time access to files/emails
- Block access to print files
- Delete or edit messages after they have been sent

Inbound Protection

Stay protected from malicious links and files, viruses, phishing and spoofing attacks, ransomware attacks and even Spam.

Multi-Factor Authentication

on the recipient- You can choose to lock an email by adding a pin or a question that can only be unlocked by the intended recipient for an extra layer of protection

No Log-in Portal or Account Necessary

one click authenticate and decrypt allows your recipients to open your emails and also reply encrypted without ever having to sign up or login to anything

Contact Trustifi today to discuss how your law firm can improve its email security. Trustifi can help your firm keep more clients and ensure them that their confidential information will never be leaked.

www.trustifi.com
1-844-235-0084
info@trustificorp.com