



Lawyerist

Top Trends in Ethical Cybersecurity

with
Jeffrey Schoenberger
jeff@lawyerist.com

NJSBA | NJICLE | NJSBF

ABOUT | NEWS | CONTACT

LOG IN | JOIN NOW









NJSBA

Resources | CLE | CLE On-Demand | Meetings & Events | Career Center | Membership | My Links/Handbooks | CLE Records

NJSBA PRACTICEHQ

The New Jersey State Bar Association's Practice HQ is a free member resource designed to help you build and maintain a successful, thriving legal practice.

Look around to find checklists, whitepapers, videos, and other resources available to you as a NJSBA member. Take a video tour [here](#).

 Opening/Closing Firm	 Client Development	 Documents	 Technology
 Money	 Management	 Comparison Charts	 Learning Library

DISCLAIMER: Practice HQ is offered as a helpful resource to members of the New Jersey State Bar Association to provide practical guidance for your practice. Information provided here, however, does not constitute legal advice, and the NJSBA makes no representations about the ethical implications of any information provided when applied to your particular circumstances. As a reminder, you should be guided by your own judgment and are ultimately responsible for ensuring your actions are consistent with the relevant applicable ethical rules.

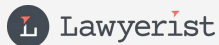
CRIME

Why Cybercriminals Are Targeting Law Firms

The legal sector proves to be vulnerable to cybersecurity risks, as more companies are attacked for sensitive data.



**...because that's where
the money is.**





**Over 200 million
Ransomware Attacks
in 2020
(Every 14 Seconds)**

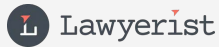


**Over 500 million
Ransomware Attacks
in 2021**





In 2023, ransomware payments exceeded \$1.1 billion; the highest ever and first year > \$1 billion.



Ethical Rules in Play (New Jersey)

- Rule 1.6 (“Confidentiality of Information”)
- Rule 5.1 (“Responsibilities of Partners, Supervisory Lawyers, and Law Firms”)
- Rule 5.3 (“Responsibilities Regarding Nonlawyer Assistance”)



Rule 1.6(a) – Confidentiality of Information

A lawyer shall not reveal information relating to the representation of a client unless the client consents after consultation, except for (1) disclosures that are impliedly authorized in order to carry out the representation, (2) disclosures of information that is generally known.



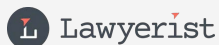
Rule 1.6(f) – Confidentiality of Information

A lawyer shall make **reasonable efforts** to prevent the **inadvertent or unauthorized disclosure** of, or unauthorized access to, **information relating to the representation of a client**.



Rule 1.6 – Confidentiality of Information, Comment

Paragraph (f) **requires a lawyer to act competently to safeguard information**, including **electronically stored information**, relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision...



Rule 1.6 – Confidentiality of Information, Comment

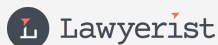
The **unauthorized access to**, or the inadvertent or unauthorized disclosure of, confidential information relating to the representation of a client **does not constitute a violation of paragraph (f) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered** in determining the reasonableness of the lawyer's efforts include, but are not limited to, the **sensitivity of the information**, the **likelihood of disclosure** if additional safeguards are not employed, the **cost of employing additional safeguards**, the **difficulty of implementing the safeguards**, and the **extent to which the safeguards adversely affect the lawyer's ability** to represent clients (e.g., by making a device or important piece of software excessively difficult to use)....



Rule 1.6 – Confidentiality of Information, Comment

A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.

...



Rule 5.1 – Responsibilities of Partners, Supervisory Lawyers, and Law Firms

(a) Every law firm, government entity, and organization authorized by the Court Rules to practice law in this jurisdiction **shall make reasonable efforts to ensure that member lawyers or lawyers otherwise participating in the organization's work undertake measures giving reasonable assurance that all lawyers conform to the Rules of Professional Conduct.**

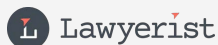
(b) A lawyer having direct supervisory authority over another lawyer **shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.**



Rule 5.1 – Responsibilities of Partners, Supervisory Lawyers, and Law Firms

(c) **A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:**

- (1) the lawyer **orders or ratifies the conduct involved;** or
- (2) the lawyer having direct supervisory authority over the other lawyer **knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.**



Rule 5.3 – Responsibilities Regarding Nonlawyer Assistance

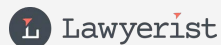
With respect to a nonlawyer employed or retained by or associated with a lawyer:

(a) every lawyer, law firm or organization authorized by the Court Rules to practice law in this jurisdiction **shall adopt and maintain reasonable efforts to ensure that the conduct of nonlawyers retained or employed by the lawyer, law firm or organization is compatible with the professional obligations of the lawyer.**



Rule 5.3 – Responsibilities Regarding Nonlawyer Assistance

(b) a lawyer having direct supervisory authority over the nonlawyer shall make **reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer;** and



Rule 5.3 – Responsibilities Regarding Nonlawyer Assistance

(c) **a lawyer shall be responsible for conduct of such a person** that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

- (1) **the lawyer orders or ratifies the conduct involved**; or
- (2) the lawyer has direct supervisory authority over the person and **knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action**; or
- (3) the lawyer has **failed to make reasonable investigation of circumstances that would disclose past instances of conduct by the nonlawyer incompatible with the professional obligations of a lawyer, which evidence a propensity for such conduct.**





“

80% of ransomware attacks originate with phishing

”

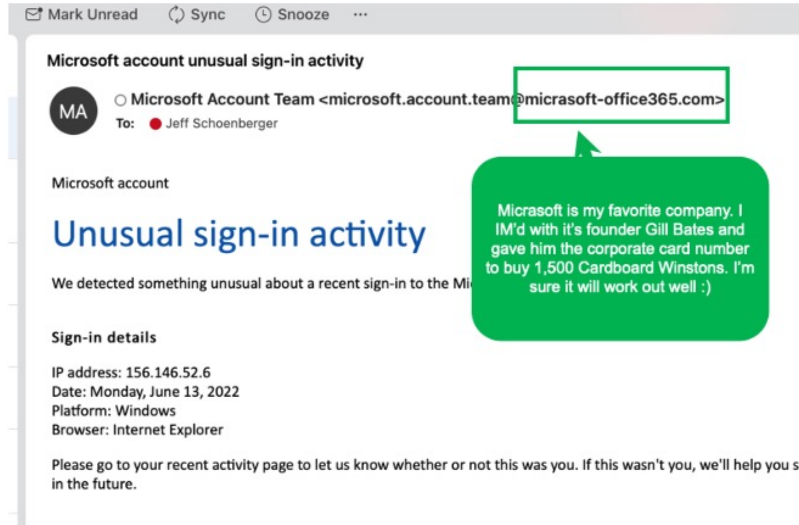


User Education

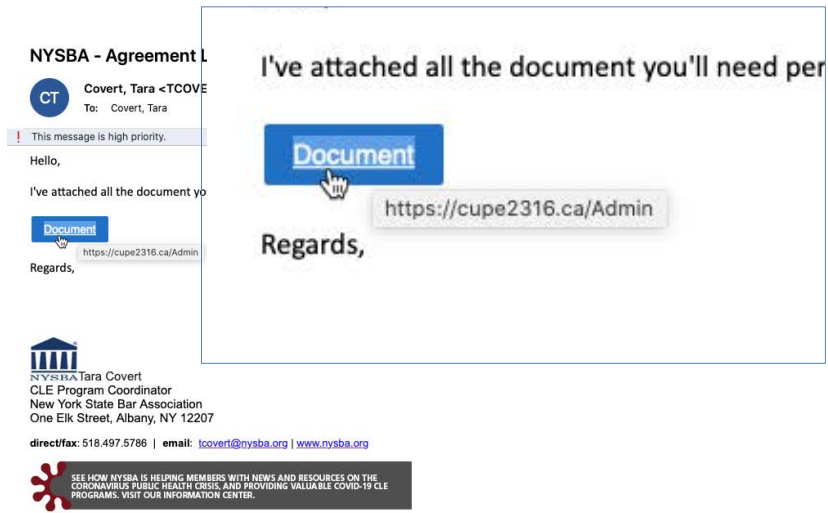
User Education Assistance



Phishing

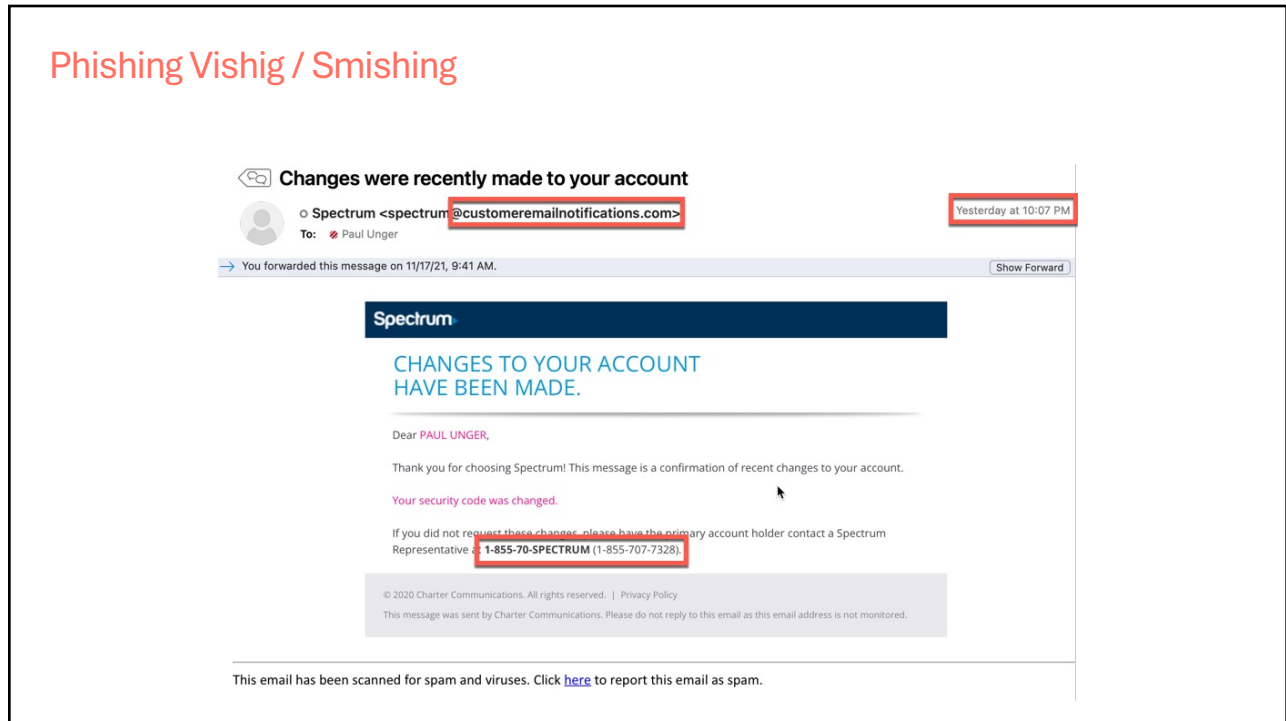


Phishing



This email has been scanned for spam and viruses. Click [here](#) to report this email as spam.

Phishing Vishig / Smishing

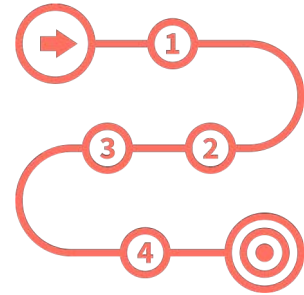


Call a number that you have in your records or on the company's main website to investigate if the email/text is legitimate.



Simple Guidelines

- Phishing Scams “Target” Everyone
- Don’t Click on Unknown Links
- Call Before you Click
- Imposters are Tricky
- Be Slightly Paranoid

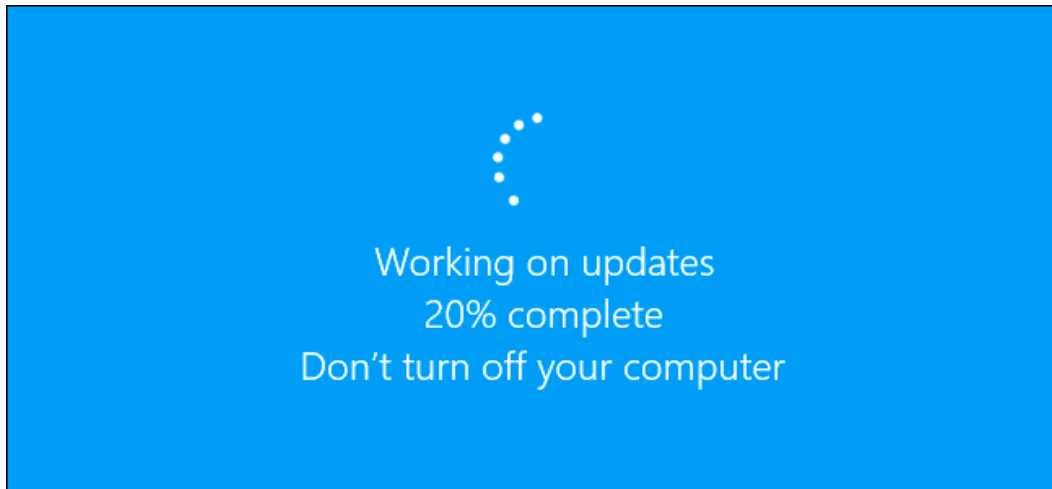


2

Shadow IT
(or unmanaged devices)



Automated OS and Program Updates



Modern Antivirus / Antimalware

- Carbon Black
- Deep Instinct
- Legacy Applications
 - AVG
 - Malwarebytes
 - McAfee
 - Norton 360
 - Windows Defender





Common Mistakes

- No Backup at all!
- Backup is untested and may not be working.
- Backups are only stored locally.
- Thinking Dropbox, etc. is a backup.





Backup ≠ Sync



Recommendations – The Best Protection from Ransomware Attacks

- No Excuses! Every Day!
- Backup Everything – Not Just Data
- Check the Logs Regularly
- Secure Offsite Copy (Web-based Great)
- Run Test Restores
- **Immutable Backups or Object Lock**



Backup for Solos or Small Firms

- Unlimited Storage
- Backup to the Cloud
- Encrypted
(user-selected password, if desired)
- App Access
- Windows and Mac

 **Backblaze**
CARBONITE[®]
an **opentext**™ company



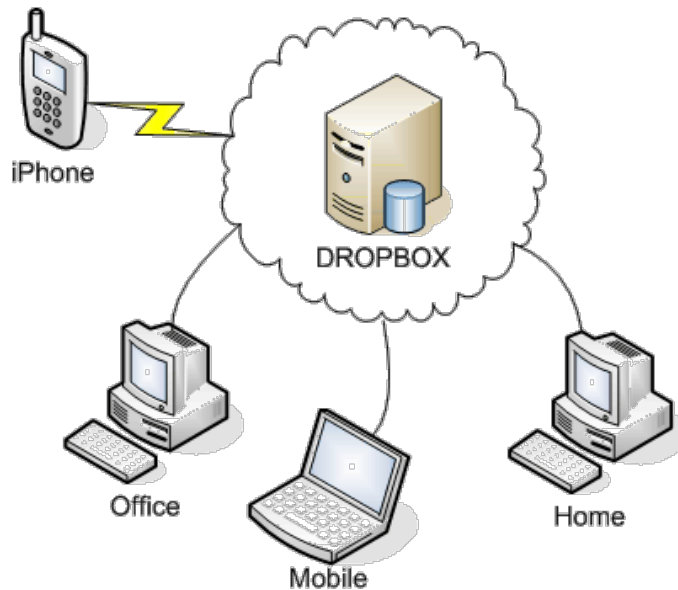
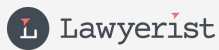
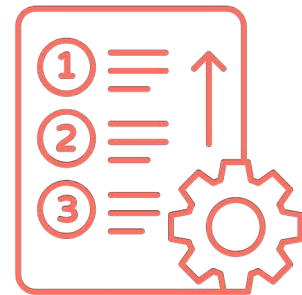
 Lawyerist

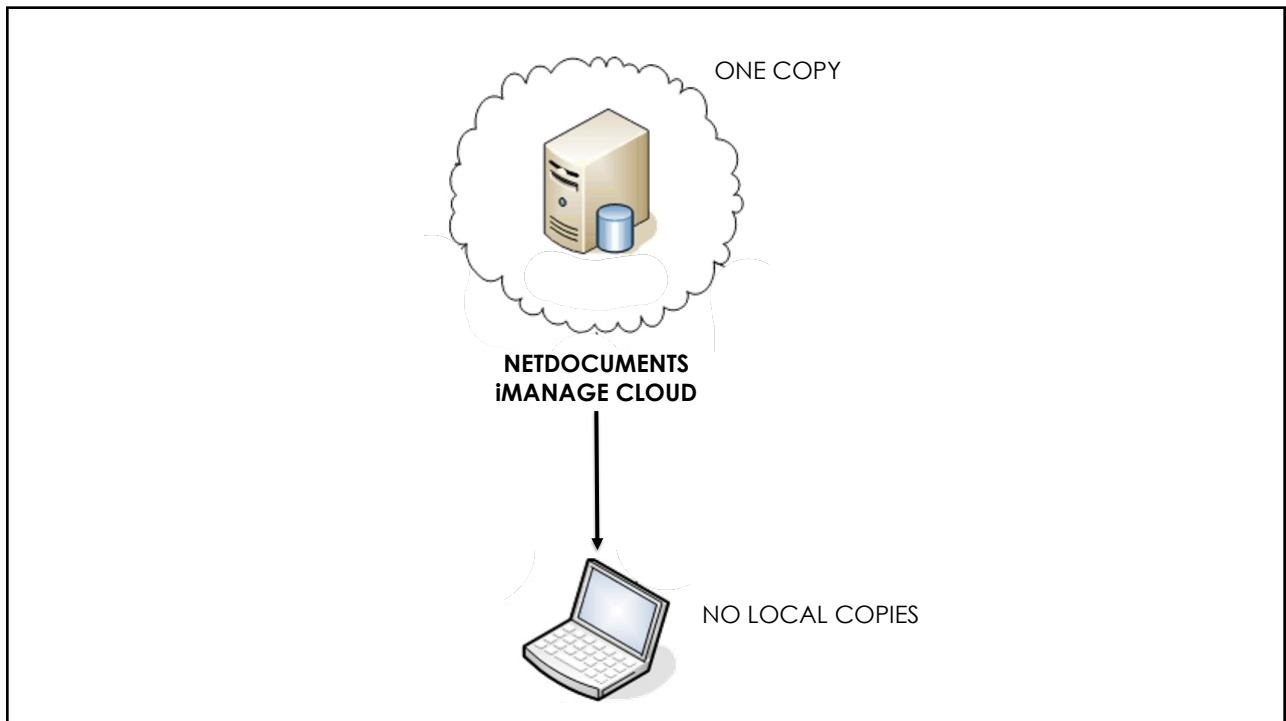
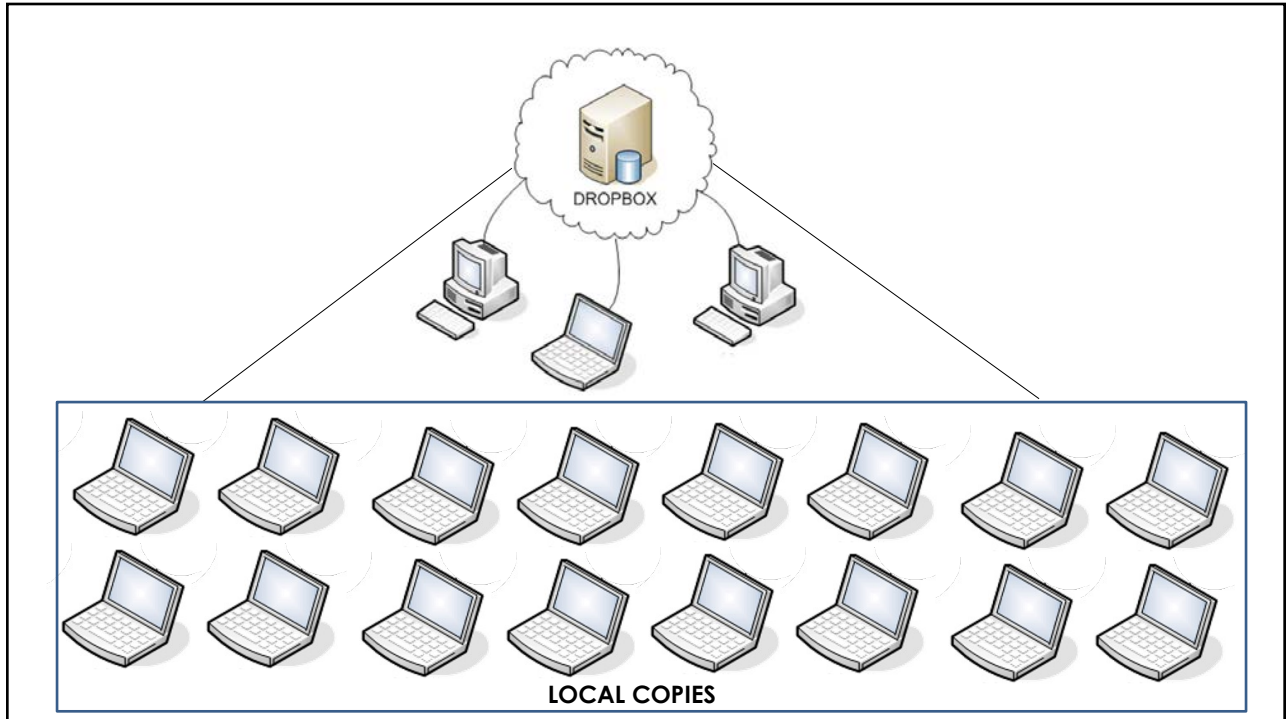


Cloud Benefits

Security Gains

Centralized, Trackable,
Manageable Data





Centralized Security Data

The logo for 1Password, featuring the word "1Password" in a bold, black, sans-serif font. The "1" is a large, stylized number, and the "o" is a blue circle with a white keyhole shape inside.The logo for bitwarden, featuring a blue shield icon with a white keyhole shape inside, positioned above the word "bitwarden" in a blue, lowercase, sans-serif font.The logo for dashlane, featuring a green shield icon with a white keyhole shape inside, positioned above the word "dashlane" in a green, lowercase, sans-serif font.The logo for RoboForm, featuring a green robot head icon with two white eyes, positioned to the left of the word "RoboForm" in a bold, black, sans-serif font.


 Lawyerist

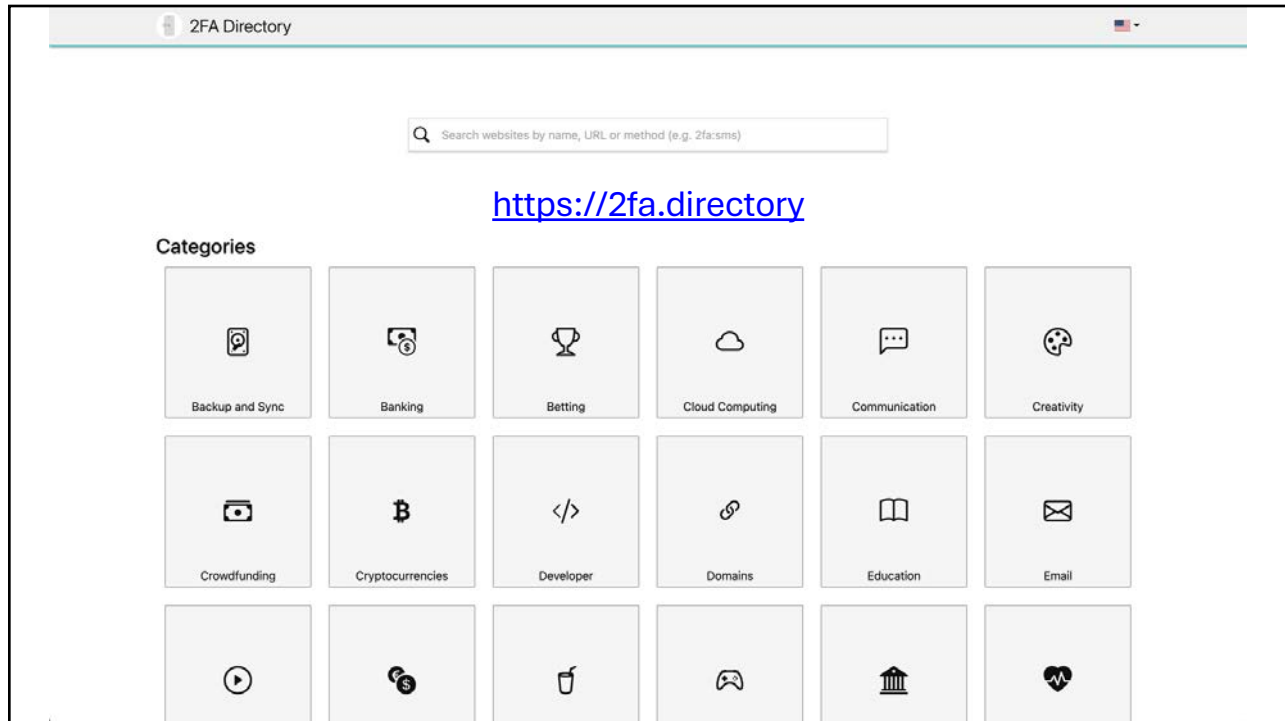
Verify with 2-Factor Authentication

Requires 2 authentication factors to verify identity:

- **Knowledge factors** – something you know
- **Possession factors** – ID card, security token or smartphone
- **Inherence factors** – biometrics

Passkeys are up-and-coming, but not yet a 2FA replacement.

 Lawyerist



“

“The cloud is a name for someone else’s computer and you need to understand how much or how little you trust that computer.” – Bruce Schneier

”



Hard Drives

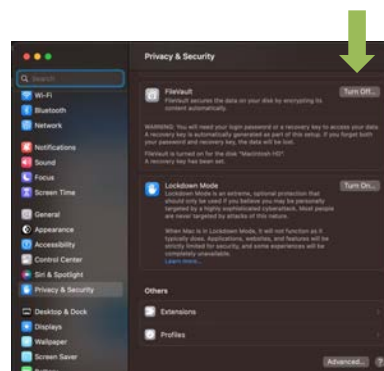
Windows BitLocker


- Windows Key > type “BitLocker” > open Manage BitLocker
- Turn on Windows BitLocker



macOS FileVault

- System Settings > Privacy & Security
- Turn on FileVault








[Products](#)
[Services](#)
[Solutions](#)
[Company](#)
[Support](#)
[Blog](#)

Shop

Home > Encrypted External Drives

SECUREDRIVE® EXTERNAL ENCRYPTED USB DRIVE




SecureData's award-winning SecureDrive® devices offer unmatched protection for your most sensitive data while it's in use, in offline encrypted backups, or on the move. Our managed and unmanaged solutions safeguard regulated or confidential information from unauthorized access. Our innovative security features keep you in control of when, where, and by whom your data is accessed.







SecureDrive® BT

SecureDrive® KP

SecureDrive® DUO

SPECIFICATIONS						
Storage Capacity	250 GB - 20 TB		250 GB - 20 TB		250 GB - 20 TB	
Dimensions (mm)	Slim ¹ 125×77×12.5	Standard ² 125×77×12.5	Slim ¹ 125×77×12.5	Standard ² 125×77×12.5	Slim ¹ 125×77×12.5	Standard ² 125×77×12.5
FIPS certification						
FEATURES						
Dishant Kaushal						








[Products](#)
[Services](#)
[Solutions](#)
[Company](#)
[Support](#)
[Blog](#)

Shop

Home > Encrypted Flash Drives

SECUREUSB® ENCRYPTED FLASH DRIVES




SecureData's award-winning SecureUSB® encrypted usb drives give you easy portability and unmatched data security for your most sensitive information. Our managed and unmanaged options give you comprehensive protection, easy portability, and confidence that your most important data is secure at rest or on the go.






SecureUSB® BT

SecureUSB® KP

SecureUSB® DUO

SPECIFICATIONS						
Storage Capacity	8 GB - 256 GB		8 GB - 256 GB		8 GB - 256 GB	
Dimensions (mm)	with sleeve 56×20×10	without sleeve 55×20×10	with sleeve 78×20×10	without sleeve 77×20×10	with sleeve 78×20×10	without sleeve 77×20×10
FIPS certification						
FEATURES						
Dishant Kaushal						





**...but, don't use USB
flash drives if you can
avoid it.**

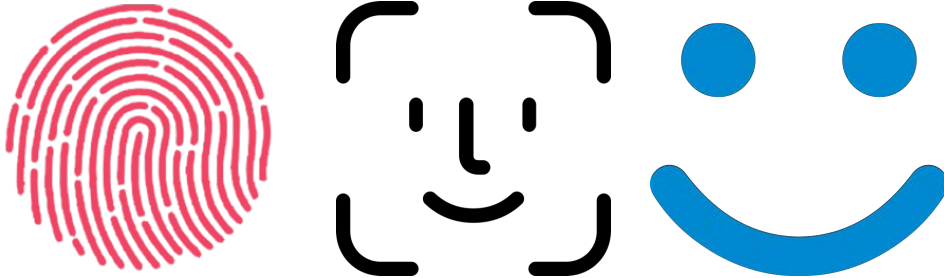


USB Flash Drives are Security Risks

Booby-trapped flash drives
can destroy hardware & networks.

They are easy to lose or steal.

Biometrics



 Lawyerist

Email



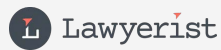
 Lawyerist

Encrypt Your Synced Cloud



CRYPTOMATOR

[Alternative to Boxcryptor](#), the former recommendation that was purchased by Dropbox



Secure WiFi for Remote Workers

WPA2 or WPA3 (or WPA3-ready)

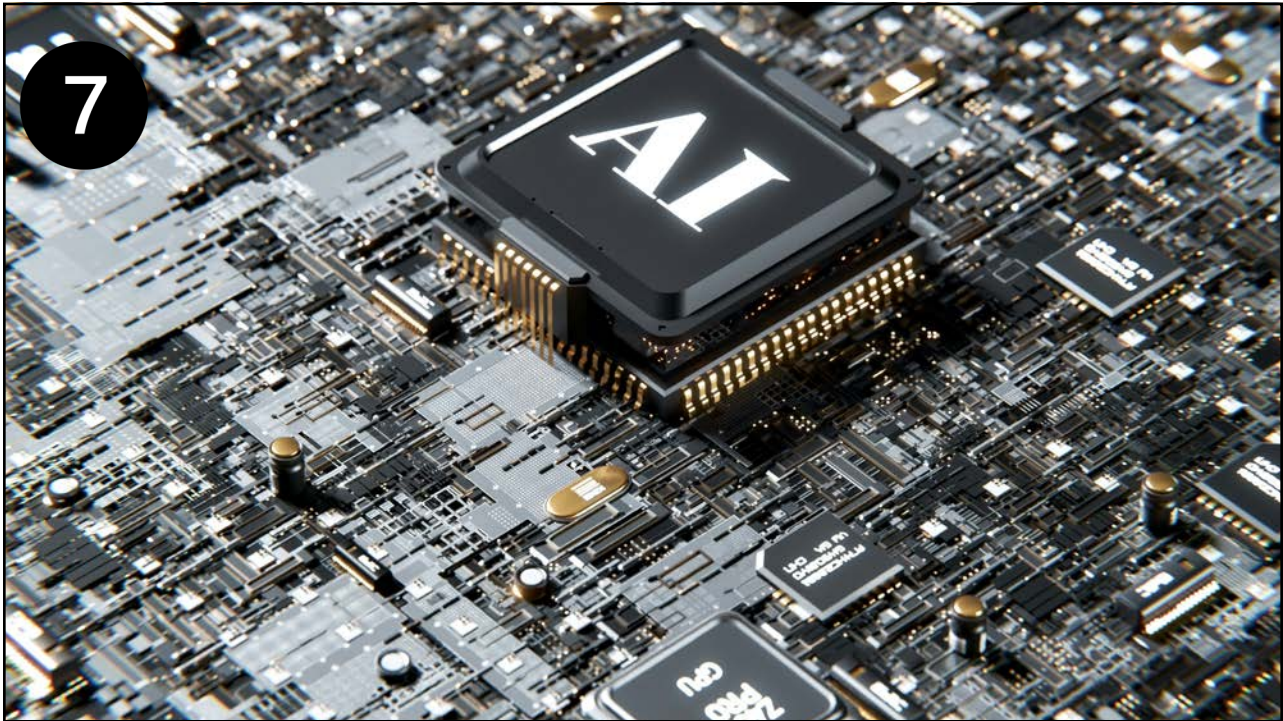




Free Options





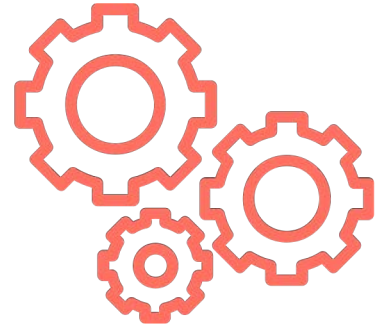


What is AI?

AI refers to the simulation of human intelligence in machines that are programmed to think and learn like humans. The term can also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving.

Key Characteristics

- Learning
- Reasoning
- Problem-Solving
- Perception
- Language Understanding



What is Generative AI?

Generative AI is a type of artificial intelligence that uses algorithms to generate new data from existing data. It can be used to create new images, music, and other forms of media.

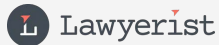
Defining Generative AI

Generative Pre-Trained Transformer (GPT)

Created to function like a human brain, trained on input, such as large data sets, to produce outputs (answers to questions)

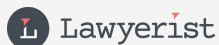
Generative AI

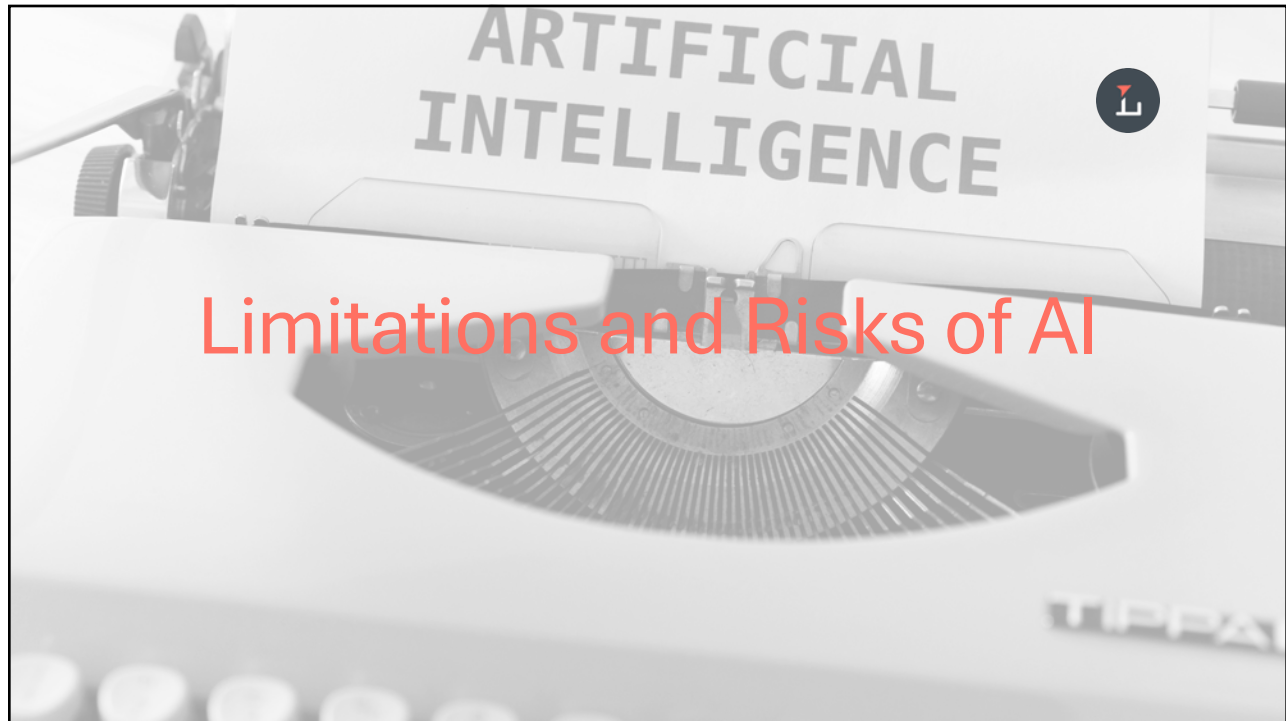
Learns patterns and structure of input to generate new data that has similar characteristics



So far, AI does what computers have always done.

It just has a bigger data set and does it much faster.





Limitations of AI

- AI is only as good as the data it can analyze.
- AI is only as good as the prompt.
- AI is only as good as how it is programed to respond to the prompt

THE WALL STREET JOURNAL

World Business U.S. Politics Economy Tech Markets & Finance Opinion Arts Lifestyle

ChatGPT Can Give Great Answers. But Only If You Know How to Ask the Right Question.

That's why companies are hiring 'prompt engineers'—experts in talking to AI systems effectively

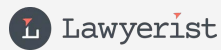
By Jackie Snow
Updated April 12, 2023 at 11:00 am ET

🔗 📌 🔍 🗨️ 20 📄 Gift unlocked article 🎧 Listen (8 min) ⋮



Risks of AI

- Data Breaches
- Model Theft
- Data Poisoning
- Privacy Violations
- Decision Manipulation



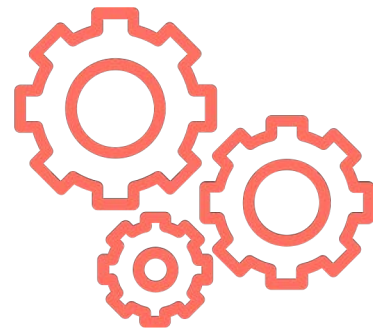
Most AI Products

- Trained on input from large data sets from the Internet – case law, treatises, websites, etc.
- Learns the patterns and structures of language.
- Produce outputs
- Uses what it learns about the patterns and structures of language to answer questions.

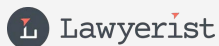


Chat-type Products in Law Practice Management Programs

- Clio (Clio Duo)
- Filevine (AIFields, DemandsAI, ImmigrationAI, SidebarAI)
- LEAP (LawY)
- MyCase IQ
- Rocket Matter (ChatGPT & time tracking)
- Smokeball AI (Archie AI Matter Assistant; Communicate, Intake)



Clio Duo

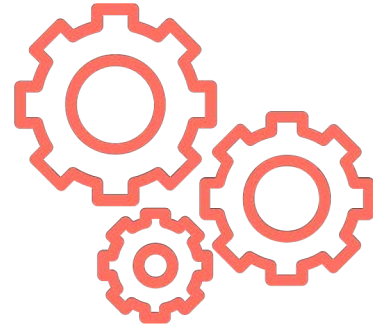


Clio Duo

The screenshot displays the Clio Duo user interface. On the left is a dark sidebar with navigation options: Dashboard, Calendar, Tasks, Matters, Contacts, Activities, Billing, Online payments, Accounts, Documents, Communications, Reports, App Integrations, and Settings. Below these are options for "Try out Automated workflows" and "Resource center" with a user profile for Jeffrey Schoenberger. The main area features a search bar and a large AI chat window titled "Ask Duo". The chat window says "Hello Jeffrey! How can I help today?" and offers actions like "Create", "Catch up on a matter", "Help me write", "Ask a question", and "Analyze documents". A text input field contains "Bring me up to speed on Bugs Bunny's matter." Below the chat is a circular progress indicator showing "0 Hours" and "1.9 Hours". The background dashboard includes a "Have feedback about Clio Duo?" button, a matter card for "00134-Kelly2018", a "Calendar Events" section with two items, and a "Billing Metrics for Firm" section with two cards: "Draft Bills 17" with a "Total in Draft" of "\$22,187.00", and "Unpaid Bills 31" with a "Total in Unpaid" of "\$28,072.05".

What can you ask Clio Duo?

- Access matter details
 1. Get me up to speed on the John Doe matter.
 2. List open matters with user John Doe as the responsible attorney
- Retrieve client information
 1. Show me recent email communications for John Doe.
 2. Retrieve contact details for John Doe.
- Find documents within a matter
 1. Which documents have been recently uploaded for John Doe's matter?
- Get caught up on case details
 1. What was the latest note about the John Doe matter?



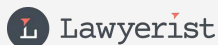
Writing a Prompt

Tone (assumed professional by system)

Sample Legal Research Prompt

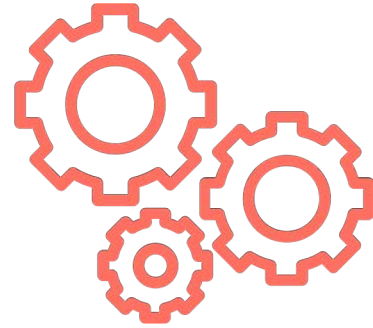
Role
Output
Purpose
Issue, including detail/context
Revision/Follow-up

- System: Lexis+ AI
- As the representative of the father, draft a legal memo about the constitutionality of a putative father registry that denies legal status of the father if not registered within 15 days of a child's birth. In this case, the mother suffered from post-partum depression and the father was the sole caregiver for the child for three weeks. The mother later took the child and disappeared for three weeks, refusing to answer the father's communication attempts. The mother put the child up for adoption, and the father seeks to intervene in the adoption. (Select jurisdiction in separate field)
- Follow up: Draft a list of counter arguments for a persuasive document.



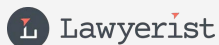
What can you ask Clio Duo?

- Access matter details
 1. Get me up to speed on the John Doe matter.
 2. List open matters with user John Doe as the responsible attorney
- Retrieve client information
 1. Show me recent email communications for John Doe.
 2. Retrieve contact details for John Doe.
- Find documents within a matter
 1. Which documents have been recently uploaded for John Doe's matter?
- Get caught up on case details
 1. What was the latest note about the John Doe matter?



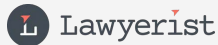
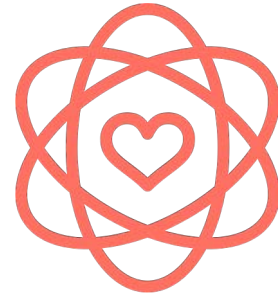
Westlaw Precision with CoCounsel

Westlaw Precision™



Westlaw Precision Features

- **AI-Assisted Research:** Answers to legal queries, accompanied by links to authoritative Westlaw sources
- **Mischaracterization Identification:** Analyzes legal documents to detect and highlight misrepresentations of cited sources
- **AI Jurisdictional Surveys:** Generates comprehensive 50-state surveys on specific legal topics
- **Claims Explorer:** Employs generative AI to match factual scenarios with applicable legal claims or counterclaims
- **KeyCite Cited With:** Identifies cases that are frequently cited together, even if they don't cite each other directly
- **Outline Builder:** Facilitates the creation of structured outlines alongside research documents



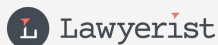
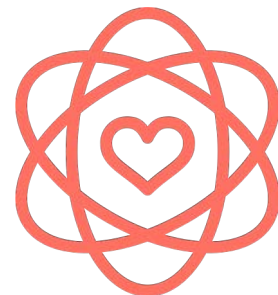
Westlaw Precision with CoCounsel

Westlaw Precision with CoCounsel Pricing

- Starting Price: \$248.95 per user per month.

CoCounsel Core Standalone Pricing

- Starting Price: \$225 per user per month.
- Volume Discounts: Available for multiple users

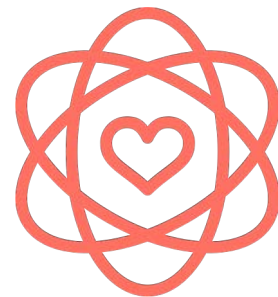


Vincent AI by vLex



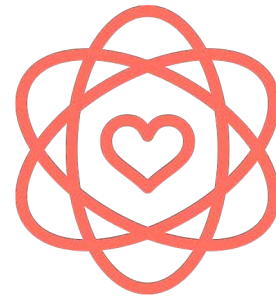
Vincent AI by vLex

- **Extract and Analyze Claims:** Outline the claims being made in the complaint, along with the citations, facts, witnesses, and parties for each claim.
- **Generate Defenses to Each Claim:** Come up with defenses to each listed claim.
- **Create Follow-up Questions for Clients:** Create a follow-up questionnaire for clients or other parties.
- **Think Through a Possible Legal Argument:** Identify and help users analyze relevant cases – its underlying LLM has the advantage of knowing the complaint and the context, and has access to vLex’s global repository of legal data.



Vincent AI by vLex

<p>Professional Plan (1 User) \$399/month</p> <p>Start a 3 Day Free Trial</p> <ul style="list-style-type: none">• No credit card required for free trial• Access to Vincent AI• Content from vLex for Federal and State courts in all 50 states• Comprehensive Data Security	<p>Small Firm (2-10 Users) \$230-270/user/month</p> <p>Start a 3 Day Free Trial</p> <ul style="list-style-type: none">• No credit card required for free trial• Access to Vincent AI• Content from vLex for Federal and State courts in all 50 states• Comprehensive Data Security• Per user discount for larger plans	<p>Enterprise (>10 Users) Contact Sales for Pricing</p> <p>Book a Demo</p> <ul style="list-style-type: none">• Access to Vincent AI• Content from vLex for Federal and State courts in all 50 states• Global Content with Vincent integrations for a host of countries• Dedicated customer support representative• Leverage customization options with vLex Labs• Single Sign-on Options• Comprehensive Data Security
--	---	---



Practice-Specific Tools

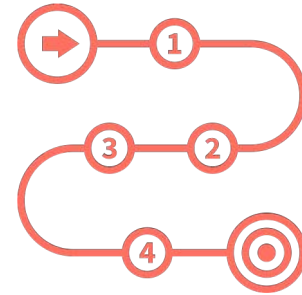
Program	Role	Features
Draftwise	Contracts	DMS-like storage and helps compare clauses, including different versions of the same clause, refine them, and mark them for frequent use. Furthermore, documents and clauses can be curated by teams or seniority and stored in collections with context tags like "Buyer Friendly" or "Seller Friendly."
LegalMation	Litigation	Helps with document generation and deposition review and analysis.
Lexis Create+	Document Creation	Streamlines the legal drafting process by combining trusted content, advanced AI tools, and seamless integration within the Microsoft 365.
Paxton AI	Contracts	Automates tasks such as contract review, legal drafting, and document analysis.
Spellbook	Contracts	Helps with review, drafting, and customization.



AI as Your
search engine

• AI Legal Learning Resources

- [How to Safely Use AI in Your Tech Stack](#)
- [Managing Your Practice with AI](#)
- [Harnessing Chat GPT in Your Firm, with Joyce Brafford from Rocket Matter](#)
- [Fair & Ethical AI, with Matthew Butterick](#)
- [Using AI to Stay Ahead, with Greg Siskind](#)



The screenshot shows the Lawyerist website interface. At the top, there is a navigation bar with the Lawyerist logo and the tagline "Guiding Healthier Small Law Firms". The navigation menu includes "Healthy Firm", "Resources", "Product Reviews", "Coaching", "About", "Subscribe", and "Account". Below the navigation bar, there is a section titled "ON THIS PAGE" with sub-sections for "Products", "How to Choose", and "Features". The main content area features a large image of a robot thinking, with a dashed line connecting it to a "More Resources" link. The main heading is "Artificial Intelligence in Law Firms". The text below the heading discusses the power of AI tools to supercharge law firms, while also noting limitations and the need for responsible use. At the bottom of the page, there is a red link titled "Directory of Lawyer-focused AI Tools".

Lawyerist
Guiding Healthier Small Law Firms

Healthy Firm ▾ Resources ▾ Product Reviews ▾ Coaching About Subscribe Account ▾

ON THIS PAGE

Products How to Choose Features

Home • Products & Services for Small Law Firms • Artificial Intelligence in Law Firms

Get the [Field Guide to Buying Products & Services](#)

[More Resources](#)

Artificial Intelligence in Law Firms

Artificial intelligence tools have the power to supercharge your law firm and save you money as you increase your efficiency, productivity, and capabilities. But these tools come with limitations, and when used improperly, they could lead to security problems, hallucinations, or just plain stupidity. Modern firms, however, can't afford to just sit and wait for AI to mature. Lawyers need to understand the tools, their uses, their problems, and their potential. Below is a collection of AI tools that lawyers and law firms may use. Some are specific to the legal field, while others are made available to the general public. Use this portal to help you responsibly navigate emerging AI tools and features.

[Directory of Lawyer-focused AI Tools](#)



Jeff@lawyerist.com

(the key is to get started)

FOLLOW A 3-2-1 BACKUP STRATEGY

All data storage systems will eventually fail. This includes the spinning hard drives in your servers or desktop computers, the solid-state drives (SSDs) in your laptop computers, and the flash memory modules in your tablets and smartphones. The question isn't "if" but "when" will you have a data storage failure.

PROTECT YOUR DATA BY FOLLOWING THIS SIMPLE RULE

- Have at least 3 independent copies of your data.
- Store the copies on 2 different types of media.
- Keep 1 backup copy offsite.

HOW TO IMPLEMENT A 3-2-1 BACKUP

The three independent copies usually mean one original (on your hard drive or server) and at least two backups. The two backups should be on two different types of media. Each media type has its vulnerabilities. If you keep backups on the same kind of media, such as external hard drives, the risk of failure is higher than if the backups are on different media types, such as one backup on an external hard drive and another in the cloud.

If you have a local backup on an external hard drive or network-attached storage (NAS) device and a remote backup with a reputable cloud backup service, you not only satisfy the second rule about using different types of media, but you also satisfy the third rule about having a backup offsite.

WHY 3-2-1 IS A BEST PRACTICE FOR BACKUP

The 3-2-1 backup rule is a best practice because it ensures you'll have a copy of your data no matter what happens. Multiple copies prevent you from losing the only copy of your data. Multiple locations ensure no single point of failure and that your data is safe from fires, theft, and natural disasters, among other calamities.

ANTIVIRUS-ANTIMALWARE SOFTWARE

Commonly, users think they have computer protection software running when they really lack it, or it is outdated. While both [Windows](#) and [macOS](#) have good defenses active out of the box these days, a nice change from prior versions, threats [grow unabated](#).

For most firms, it's a good idea to supplement the operating system vendor's tools with a third-party application. Highly regarded vendors for antivirus-antimalware programs include:

- [Avast](#);
- [AVG](#);
- [Malwarebytes](#);
- [McAfee](#); and
- [Norton](#).

You may need to consult an expert. I use Malwarebytes, which I like. But, of course, there are many good options available from vendors. A good security suite provides antimalware, antivirus, web protection, vulnerability testing (to make sure you have the latest versions of programs that may represent vulnerabilities), a firewall, intrusion detection, antispam and ransomware protection.

SECURE FILE SHARING AND DATA ROOMS

Sharing data through known-safe spaces reduces the likelihood of a virus or malware infection. How? Because firm users have an easy and controlled way to request files from and send files to clients and other outside parties. Random, unexpected attachments are no longer a "sure, let's click on this" attraction because, instead, files come and go through one secure, expected way.

Caveat: When using a service below, ensure all shares have a password to access them.

ANSARADA VIRTUAL DATA ROOM

See <https://www.ansarada.com/features/data-rooms>.

BOX.COM

See <https://www.box.com/pricing>.

DROPBOX STANDARD OR ADVANCED

Standard is \$15/user/month, and Advanced is \$24/user/month. For an explanation of their business plans, see <https://www.dropbox.com/business/plans-comparison>.

FIRMEX VIRTUAL DATA ROOM

See <https://www.firmex.com/>

GOOGLE WORKSPACE

The [Business Starter](#) plan is \$6/user/month and includes 30 GB of cloud storage; the Business Standard plan is \$12/user/month and has 2TB of cloud storage.

INTRALINKS VIRTUAL DATA ROOM

See <https://www.intralinks.com/products/mergers-acquisitions/virtual-data-room>

MICROSOFT 365 OR ONEDRIVE FOR BUSINESS

OneDrive is Microsoft's cloud storage offering and comes with nearly every Microsoft 365 plan. For only \$6/user/month ([Business Basic plan](#)), you get 1 TB of online storage.

ONEHUB

See <https://onehub.com>.

SHAREFILE BY CITRIX

See <https://www.sharefile.com/>. ShareFile is a fantastic service that allows you to securely create virtual "rooms" for others and share documents with them. You decide what rights each user has to the collection of documents.

SMARTROOM VIRTUAL DATA ROOM

See <http://smartroom.com/>.

SYNCPPLICITY

See <https://www.syncplicity.com/>.

BACK IT UP!

By Barron K. Henley, Esq. and Jeffrey Schoenberger, Esq.

DON'T CUT CORNERS HERE

Backup is not an area to cut corners on costs, but there are ways to protect yourself and not spend extravagantly.

BACKUP DEVICE/SYSTEM OPTIONS

We recommend that your primary backup is internet-based, constantly running as a background process on your machines. However, we do NOT recommend relying solely on an Internet backup option. Have a secondary backup system on-site (either external hard drive(s) or network-attached storage (see below)) Here are a few suggestions:

INTERNET BACKUP OPTIONS

This is becoming common as the primary backup method. The biggest advantages of internet-based backups are that they are offsite, someone else handles all hardware issues, and your files are backed-up to highly-secured data centers with redundant power and internet. Top vendors in the field are:

- [Backblaze](#);
- [CrashPlan](#);
- [Carbonite](#); and
- [SOS Online Backup](#).

No matter what you do, you must get a backup system. It is not optional. Losing all your data can cripple your practice and cause you to commit malpractice. The risk is simply not worth it.

EXTERNAL HARD DRIVES

There are external hard drives explicitly designed as backup devices, and this is our recommendation. They hold tons of data and are inexpensive. The annoyance is that you must unplug one of them and take it home with you daily (they need to be rotated so you always have one complete, local backup offsite). On the other hand, they're speedy and reliable. Look for at least 5 TB of storage and a 7,200 rpm drive. If your computer supports USB-C or Thunderbolt, look for drives allowing you to take advantage of the faster speeds those interfaces offer. There are many options.

NETWORK ATTACHED STORAGE ("NAS")

Without getting too technical, NAS is storage (usually an external hard drive) attached directly to your network rather than to an individual PC or server. The benefit is that all computers connected to the network can access the NAS regardless of which computers are on or off. Furthermore, higher-end NAS devices employ RAID (Redundant Array of Independent Disks). RAID is a configuration in which multiple hard drives are arranged to store data across all of them simultaneously. Even though multiple drives are involved, your computer sees the RAID as a single drive letter on the network. RAID gives you better performance (surprisingly), capacity, and reliability than a single large drive. There are several "levels" of RAID, including RAID 1 (straight mirroring when two drives both contain the same data) and RAID 5 (Rotating Parity Array - all data is distributed across all drives, and there are at least 3). For a good explanation of RAID and what the levels mean, see <https://en.wikipedia.org/wiki/RAID>. It can contain multiple backups of your data, and if RAID is employed in the device, it's improbable that you'll have a simultaneous crash of all the drives contained inside the NAS.

BENEFITS AND DRAWBACKS OF A NAS

NAS devices run the gamut in terms of price and capability. They can be as simple as a hard drive connected to your wired network or as complex as a server that hosts documents, websites, and even virtual machine computers. But, of course, as you add capabilities, you add cost, complexity, and potential security risks.

The primary benefit of a NAS is easy sharing and backing up of documents you do not want to store in a cloud-based sync service. However, except for [Tresorit](#), every major cloud storage vendor can turn over readable data if it is served with a subpoena or lawful warrant. This is true of Apple's iCloud, Dropbox, Google Drive, and Microsoft's OneDrive. Whether you're provided notice and an opportunity to contest depends on the service and its terms of service. It's possible to add your own, known-only-to-you, encryption to these major services, except iCloud, via [Cryptomator](#), but by default, all client data you store in these cloud services has the potential to be produced upon request in a readable fashion.

Files that you store on a NAS are triply protected from this outcome.

- First, the files are stored in a device that you control. If you want the hard drives encrypted with a password only you know, you can do that.
- Second, while it's possible to configure a NAS so that you can access your files from outside your network (*e.g.*, on your smartphone via a mobile app), you don't have to activate that feature, and if you do, the data doesn't live on an intermediary server "in the cloud" somewhere; it still lives on the NAS. Although accessing NAS files over the internet does mean that those files transit through an intermediary server owned and controlled by the NAS vendor, they don't reside there. The vendor's server is a mere bridge, not a filing cabinet or data warehouse.
- Third, the physical NAS device lives in a location you own or control (*e.g.*, your home or office). To access the files, the interested party must gain access to your premises. And, of course, Fourth Amendment search and seizure law is much better developed than interpretive standards for terms of service policies for cloud vendors.

Having presented the "pro" case for NAS devices, one must be aware of the "cons" as well.

- First, a NAS is a computer. Depending on the features you want, like accessing documents over the internet, it is also a server. It runs an operating system and applications. Like your Mac or Windows computer, that operating system and those applications must be kept up-to-date for maximum security. Fortunately, most NAS products are designed to keep themselves updated automatically, much like our smartphones and apps.
- Second, you must practice good security hygiene for a NAS connected to the internet. This means a complex password and, if available, multi-factor authentication for any remote access. Many people never change the username and password combination to their internet router, which is often the same for every device provided by a given cable company or internet service vendor. Don't be the person who loses client files because someone tried the NAS vendor's default username and password successfully to gain access to your NAS.
- Third, although vendors have improved their software markedly in recent years, granting a NAS access to and through your network to the internet harbors the risk of opening a gateway that lets bad people in. If you are uncomfortable making changes to your internet router or have no idea what an IP address is, think twice before going with a NAS.
- Fourth, one of the chief benefits of a NAS, that the device and hence the files are under your physical control, is also a negative because that means the device is as vulnerable to theft, fire, or other disasters as the items in your home or office. If the NAS is your backup and it is destroyed, that's bad news for the business. Fortunately, it is possible to configure a NAS for automatic, unattended backups to the cloud. Those cloud backups can be encrypted with a password you set, so you get the benefits of the NAS and the protection of offsite backup without risking exposure of client information.

If you're interested in further research on a NAS device, here are three major vendors to get you started:

- [Buffalo](#);
- [Synology](#); and
- [Western Digital](#).

RECOMMENDATION REGARDING BACKUP HARDWARE AND SOFTWARE

If you just want to ensure your laptop or desktop is getting backed up, it's hard to beat Carbonite's Personal Plus plan for ~\$85/year. Buy any external hard drive and Carbonite will back up your files to their secure cloud servers and make a complete mirror of your internal hard drive on the external drive you connect simultaneously. Further, it works in the background to ensure everything is backed up, and you don't have to remember to do anything.

BEST PRACTICES FOR HARDWARE MAINTENANCE

RECORD GENERAL DETAILS ABOUT YOUR HARDWARE

THE COMPUTER'S SERIAL NUMBER

Windows: There is often a sticker on the underside of the computer (for laptops) or the back of the computer (for desktops). If there is no sticker, or it is unreadable, you can obtain the same information typing **wmic bios get serialnumber** in a command prompt window.

Macs: Click on the Apple menu and select About This Mac. See this [help article](#) for additional information.

CONTRACT NUMBER AND CONTACT INFORMATION FOR ANY EXTENDED WARRANTY CONTRACT

Windows: The manufacturers have different names for support contracts. Lenovo calls them "Premier Support." Dell calls them "ProSupport" and "ProSupport Plus." Coverage terms run from one to five years. The top-tier contracts provide that a repair technician comes to your location within 24 hours.

Macs: Apple's extended support contracts are "AppleCare," which is available as a monthly or one-time purchase for a maximum of three years. Apple does not offer onsite repair technicians, relying instead on their network of retail stores.

For both types of computers, if you bought the machine and extended warranty simultaneously, the contract and machine are usually linked at the time of purchase. It's best to buy a manufacturer's extended support offering over one offered by a store or retailer.

MAC ADDRESS OF COMPUTER

The MAC address consists of six pairs of letters and numbers separated by colons. An example MAC address is 2C:54:91:88:C9:E3. Any computer connected to a network has at least one MAC address. The MAC address marks it as a unique endpoint on the network. A computer having both an ethernet (wired) option and a WiFi (wireless) option will have two MAC addresses, one for each method of connecting to a network.

MAC is shorthand for Media Access Control. The MAC address is the location or "address" of your device on the network. Every networked device has a MAC address. MAC addresses are not limited to Apple's Macintosh (Mac) laptops and desktops (note the difference in capitalization). Windows machines have MAC addresses, so do Chromebooks, smartphones, tablets, internet-connected TVs, and streaming boxes like Roku and AppleTV.

Windows: Find your MAC address by right-clicking the Start menu, then select Network & internet. For wired connections, select the Ethernet sub-menu, then scroll down to find the MAC address. For wireless connections, select Wi-Fi, then Hardware properties.

Macs: Open System Settings (in macOS 13 Ventura) or System Preferences (versions prior to macOS 13 Ventura). Then select your connection method (*e.g.*, Wi-Fi), then click Advanced.

OPERATING SYSTEM THE MACHINE USES

Windows: Your computer likely runs either Windows 10 or Windows 11. Both versions come in Home and Pro variants. Further, Microsoft often issues interstitial updates that are not mentioned in the branding. These updates come via Windows Update, which you should set to automatically run and apply updates to ensure the best security. Updates are identified by the date of their release, such as 22H2, meaning the update released in the second half (H2) of 2022. A full description of a current Windows installation might be Windows 11 Pro 22H2.

To determine your version of Windows, see this [help article](#).

Macs: Versions of the operating system are identified by a name and number. For example, in October 2022, Apple released macOS Ventura 13.0. Like Microsoft, Apple provides security and feature updates throughout a product's lifecycle. The version preceding Ventura was Monterey. Its final update was macOS Monterey 12.6.1.

To determine your version of macOS, see this [help article](#).

PRIMARY WEB BROWSER THE MACHINE USES

The default, built-in browser for Windows is [Edge](#). For macOS, it's [Safari](#). If something is malfunctioning on the computer, such as not being able to connect to the internet, check if the same thing happens with the "factory default" browser. That's one way to eliminate a variable when troubleshooting.

UPDATE YOUR OPERATING SYSTEM

UPDATE WINDOWS

Windows 10: Click the Start button, then Settings, then Update & Security, then Windows Update.

Windows 11: Click the Start button, then Settings, then Windows Update.

Additional details are available [here](#).

UPDATE MACOS

macOS 13 Ventura: Open System Settings, click General, then Software Update.

macOS 12 Monterey and Earlier: Open System Preferences, then click Software Update.

Additional details are available [here](#).

PICK AND CHOOSE YOUR STARTUP PROGRAMS

Computers run many programs at startup. The more programs the operating system must load at startup and continuously run in the background, the fewer resources are available to you, the user. Some programs, such as cloud sync utilities or antivirus or anti-malware programs, should launch at startup and run continuously. But non-essential, rarely used programs also launch at startup. Review the list of programs you run at startup.

Windows: This [article](#) explains how to check startup programs for both Windows 10 and 11.

macOS 13 Ventura: Open System Settings, click General, then Login Items.

macOS 12 Monterey and Earlier: Open System Preferences, click Users & Groups, then select your username, then click Login Items.

Additional information for Macs is available [here](#).

GENERAL HARDWARE MAINTENANCE SUGGESTIONS

CHECK ACCESSORIES FOR DAMAGE OR WEAR AND TEAR

- **Keyboard:** Clean the keyboard with a dust brush. Compressed air is also helpful for cleaning out underneath keyboard keys, especially if you eat at your desk. For laptops, you can also place the computer open sideways on your desk, like a hardcover book, and spray "down" under the keys.
- **Keyboards and Mice:** Wipe these down with cleaning and disinfectant wipes designed for electronics. Example brands are [Weiman Disinfectant Electronic Wipes](#), [Endust for Electronics](#), and products from [iKlear](#). Do not use "standard issue" cleaning products, especially those with ammonia, on electronics. Anything you use should state specifically that it is safe for electronics, LCD/LED screens, etc.

- **Bluetooth Accessories:** If your keyboard or mouse connect via Bluetooth, check their battery levels. On Windows 10/11, connect the device to the computer, then right-click on the Start button and select “Settings.” Then select Bluetooth & devices and click on the device you want to check. Battery status may also be displayed beneath the device’s name in the list. On Apple Macs, battery level information is available from the Bluetooth icon in the top right of the menu bar. Alternatively, go to System Settings (System Preferences in old versions of macOS) and select Bluetooth. Battery status will display beneath the device’s name.
- **Dust Equipment:** Dust is an enemy of electronics. It builds up on things you don’t move, like desktop computers, monitors, and docking stations. Dust blocks air vents, traps in heat, and conducts static electricity, particularly in the winter and in dry climates. Turn off the equipment and dust it with an anti-static cloth. You can also use compressed air to clean vents.

ORGANIZE YOUR CABLES

- Organize cables by color and function. With the transition to USB-C connectors, there are now numerous cables with the same connector that could offer different functions and data speeds. A cable with USB-C connectors could provide the speeds, capabilities, and limitations of USB3, USB4, Thunderbolt 3, or Thunderbolt 4. The cable could provide data or merely power a device. Keeping cables well-identified is more important than in the past, when different connection ends ensured that the “wrong” cable wasn’t connected. Connecting “the wrong” USB-C cable will not damage equipment but may prevent it from functioning properly or turning on at all.
- Make sure no cables are obstructing access to the machine.
- Make sure no cables are obstructing access to the workspace.
- Make sure all cables are in good condition. If something is malfunctioning, try replacement cables. Cables can and do wear out.

DON'T OVERCHARGE YOUR BATTERIES

Resist the temptation to keep your portable devices always plugged in. Although hardware is much better than in the past at protecting batteries from being “overcharged,” draining the battery to below 20% every so often remains a good policy. Once every month or two is sufficient.

EMAIL ENCRYPTION AND SECURE CLIENT

By: Barron K. Henley and Jeffrey R. Schoenberger

WHAT THE EXPERTS SAY

Here are a couple of quotes to consider:

"A secure email account that the attorney is assured protects the content of correspondence. No attorney should use Gmail or other free services that in fact admit that they use personal information from email content. They should encrypt their client correspondence. Before sending sensitive correspondence, they should check by phone or text with the client to see what method of delivery is preferred."¹

"The level of encryption may vary based on practice areas or, more importantly, the firms' clients. At a minimum, emails and attachments that contain confidential data should be encrypted or sent through collaboration tools that send encrypted links rather than plain text data."²

"It's all about encryption of the 3 main risk areas for data held: data in transit, at rest and in backups. It doesn't matter if it's email, Instant Messages, case files, discovery or 3rd party expert communications, the principle of encryption is the ONLY way you can really satisfy due diligence requirements."³

ENCRYPTING DATA ON THE INTERNET

BACKGROUND

We all know how convenient email is. With smartphones and tablets, we can read and respond from anywhere at a time of our choosing. Email is also one of the oldest internet technologies, predating HTML (*i.e.*, web browsing), by 28 years; 1971 vs 1989 for you history buffs. Old technologies are not ipso facto bad. Generally speaking, they are robust and adaptable; that's how they survive. But old technologies, particularly computer technologies, were developed "among friends." Neither Ray Tomlinson (who sent the first email) nor Tim Berners-Lee (the father of the world wide web) thought much about internet security. In both decades, the internet was the province of governments, academics, and other trusted individuals and institutions.

In the intervening 25 years, security has taken an infinitely more prominent role in networked computing. There's very little human interaction or business service that isn't replicated to some degree on the internet. The core technologies of HTML and email have adapted to meet those needs. With HTML, security came in the form of [SSL and then TLS](#), the technology represented in your browser's address with a padlock when you access your bank or other private site. Indeed programmers wrote a browser plugin, [HTTPS Everywhere](#), to ensure you always get a website's secure version, if one exists. Email underwent similar, but less dramatic and less consistent, changes.

¹ [Law Firm Data Security: Experts on How to Protect Legal Clients' Confidential Data](#), by Nate Lord, DigitalGuardian, October 13, 2015, quoting Robert Ellis Smith. See <https://digitalguardian.com/blog/law-firm-data-security-experts-how-protect-legal-clients-confidential-data>.

² *Ibid.*, quoting Marco Maggio.

³ *Ibid.*, quoting Steve Santorelli.

EMAIL ENCRYPTION SERVICES

While the transition to a more secure internet for websites is well underway and nearly invisible to end users who “just want to get things done,” the same is not true for secure email. A substantial roadblock to an easy, seamless transition lies in the fact that no entity controls both ends of an email exchange. In the case of secure web browsing, one can guarantee that a site visitor is using one of four or so potential browsers (Apple’s Safari, Google’s Chrome, Microsoft’s Edge, and Mozilla’s Firefox). Across all platforms (desktop, mobile, and tablet) those four account for 95% of browser usage. The shares vary based on platform and region (*i.e.*, continent or country). But in no case does a browser move from a rounding error to a front runner. [Run your own tests here](#). If those four browsers adopt a security protocol, you can implement it on your website confident that 95% of visitors will use it without a problem.

In the case of email, there’s no such unity. Email runs on three potential protocols: IMAP (Internet Message Access Protocol, an open standard), Google’s Gmail (which is IMAP-like with a bunch of Google customizations), and Microsoft’s Exchange. They each of advantages and disadvantages but they all talk to each other. When I exchange emails with someone, I don’t know what their backend email protocol is. Furthermore, I could access email through a myriad of devices, programs, and even web browsers. My company uses Microsoft 365, which includes Exchange. I use a MacBook laptop. I could access my email via Apple’s Mail desktop mail program, its iPad or iPhone companions, Outlook for Mac, or any web browser that runs on a Mac. Add in Windows and the number of potential endpoints more than doubles. Including Android devices (smartphones and tablets) increases the number further. That doesn’t even include third-party email clients on the desktop or mobile. Unlike web browsers and websites, it’s not a matter of getting four companies to agree. That leaves email communication at the lowest common denominator, in plain text and unsecured.

This security gap has led companies to develop their own utilities or add-ins that ride on top of existing email protocols. These tools, which usually come with subscription fees, encrypt the email message and attachments before it leaves your device. The message recipient receives an email, but not the email you sent. What the recipient gets is an email with a link (usually HTTPS-secured) that sends them to a website to read your message, download attachments, and reply to the message.

The options listed below are inexpensive and easy. They encrypt both the emails and any attachments to the email. In most cases, a password must be entered by the recipient to open the email and any attachments.

- A. ECHOWORX ENCRYPTED MAIL: <https://www.echoworx.com/email-encryption-platform/>
- B. HIGHTAIL: <https://www.hightail.com/> - this service was formerly known as YouSendIt.com. It’s designed for sending enormous attachments, but also offers encryption for those attachments. Incredibly easy to use and inexpensive. It does not encrypt the text of an email, only the attachments.
- C. HUSHMAIL: <https://www.hushmail.com/plans/legal/>
- D. IDENTILLECT: <https://identillect.com/> - many bar associations offer discounts on this service.
- E. MICROSOFT 365 E3 & ABOVE: <https://www.microsoft.com/en-us/microsoft-365/enterprise/e3> - Despite the name, you do not have to be a large organization to subscribe to E3. It’s more expensive, but it includes [Microsoft’s Office 365 Message Encryption](#), which allows easy email encryption from within Outlook without any extra plugin or subscription. It’s also one of the easiest for message recipients to use too.
- F. RMAIL: <http://www.rmail.com/> - registered email service which can prove delivery + encrypted email
- G. SENDITCERTIFIED: <http://www.senditcertified.com/> and note that they offer discounts through several bar associations.
- H. SHAREFILE: <https://www.sharefile.com/>

ENCRYPT EMAIL ATTACHMENTS

Word, WordPerfect and every good PDF program including Acrobat offers file encryption. This functionality is built-in so you only have to learn how to use it. With file encryption, the file simply cannot be opened without a password. You email the encrypted attachment while the body of your unencrypted simply says "Please see attached." That attached file containing the sensitive information would be encrypted on its own. The recipient needs a password to open the encrypted attachment. But remember, do not include that password in the email. Text or call the recipient with the password. Alternatively, the password could be something you and the client decide in advance, perhaps noting it in the engagement agreement.

ENCRYPTION OPTIONS FOR ONLINE SYNC PROGRAMS AND PORTABLE MEDIA

ONLINE SYNC TOOLS

It seems like everyone has an online sync program these days. If you're in the Microsoft camp, you have OneDrive. The Google camp has Google Drive. Apple has iCloud Drive. And, Dropbox, the granddaddy of online file sync, is happy to take your money irrespective of your platform choices.

One thing to keep in mind about all these online sync platforms is that a tradeoff exists between convenience (My files everywhere I am!) and security (My files are "up there" in the cloud.). Every major sync service says, and it's true, that your files are encrypted in transit from your device to their servers and back. They also tell you that your data is encrypted at rest, *i.e.*, while stored in their data center. For legal professionals, the concern with both scenarios is that vendor holds the keys to your data. If Dropbox or OneDrive is served with a subpoena or lawful warrant, they can turn over readable data to the requesting party.

A few sync services carved out a niche where you, as the end user, define a password that encrypts your data. If one of these services is served with a warrant or subpoena and they turn over your data, the receiving party still needs the password that only you know to turn the encrypted data into readable information. Sounds nice!

What you lose in the process is most of the integrations between sync services and third-party programs, particularly on mobile applications. One of the reasons some folks refer to Dropbox as the "file system for the internet" is that developers have integrated it deeply into their own programs. Even Microsoft has done this; you can open files from Dropbox in the native iOS Word, Excel, and PowerPoint programs. You don't even need the Dropbox app on your iPhone or iPad to do it.

SECURE YOUR WHOLE CLOUD

If you are comfortable putting your finger on the scale in favor of security and losing a bit of convenience, [Tresorit](#) is the cloud vendor for you. They have all the standard cloud sync features, but you can define your own password. They are price-competitive with Dropbox and iCloud Drive. Business plans start at ~\$15/user/month.

SECURE A PORTION OF YOUR CLOUD

If you prefer the convenience of Dropbox but want to encrypt a portion of your cloud storage with a password only you know, there exist a couple of encryption programs that "ride on top" of OneDrive, Dropbox, etc. The advantage of these programs is that they only encrypt with your password the individual files or folders you select. If you want most of your sync storage unencrypted, for convenience, but need a portion of "high value documents" encrypted, for security, these cloud sync value-added programs permit this. These services will effectively eliminate your ability to share files with individuals outside of your office, but they also provide complete protection for your files as they are encrypted before the sync service ever gets your files.

- Cryptomator: See <https://cryptomator.org>. Cryptomator is open-source software that you use to create a special folder called a "vault," which holds files like any other folder on your computer. That vault is password-protected with a password only you know. The vault can be stored anywhere, including the major cloud sync services.

EXTERNAL HARD DRIVE AND FLASH DRIVE ENCRYPTION

If you're uncomfortable with cloud sync storage, or you need to move a large amount of data, if the data requires encryption, then there are a couple of different routes to go.

RELY ON SOFTWARE

There are plenty of software packages that will encrypt data for you. Both Windows 11, via [BitLocker To Go](#), and macOS, via [Disk Utility](#), allow you to encrypt a removable media (e.g., hard drive or flash drives) without spending any extra money.

Going this route means that you can use any hard drive or flash drive you have lying around.

EXTERNAL USB HARD DRIVES

If you do not want to rely on software alone, you operate in a mixed PC and Mac environment, or don't know the operating system or computer situation of the data's possible recipients, several vendors make hard drives and flash drives where the encryption technology is part of the drive's physical construction. They usually have a number pad on the device and require entry of the passcode before the drive can even be seen by the computer to which it is attached.

You could also be a "belt and suspenders" person who encrypts the data via BitLocker or Disk Utility on a drive that also has hardware encryption with physical passcode buttons. The technologies do not interfere with each other.

Here are some options:

HARD DRIVES

- [Apricorn Aegis Padlock](#) external hard drives; and
- Lenovo ThinkPad USB 3.0 [Secure Hard Drives](#).

FLASH DRIVES

- Apricorn Aegis [Secure Key](#) Encrypted Flash Drives; and
- Kingston [IronKey](#) USB Flash Drives.

LEARN MORE

Visit [Lawyerist's](#) article on [small firm file management](#) to learn more about a systematic approach to safe, convenient, and secure electronic file handling.

PASSWORD MANAGERS

By Jeffrey R. Schoenberger

WHAT IS A PASSWORD MANAGER

A password manager is a program that helps one store, create and organize passwords (and logons and websites, etc.).

PURPOSE OF A PASSWORD MANAGER

The purpose of a password manager is three-fold:

1. The program helps you create and store the innumerable login credentials that we all generate. A password manager can propose super-complex, impossible-to-guess, and impossible-to-remember, unique passwords for each site requiring a login. Most password managers also offer to store ancillary data, like software license keys, credit card numbers, store rewards card numbers, and things of that nature.
2. The password manager installs a plugin in your browser and “watches” while you surf the web. If you visit a site for which you’ve already created or stored credentials in the password manager, it offers to log you in without you having to type, or even copy and paste, your credentials. If you visit a site for which you need to create a username and password, the password manager suggests strong passwords.
3. Most, but not all, password managers let you sync your data over the internet. That way those super-strong, unmemorable passwords are accessible on your smartphone, tablet, and any additional computers you have. Having those passwords stored with a third party understandably makes some folks nervous. But, unlike most cloud storage vendors, you define the password that unlocks your data. If the password syncing website suffers a breach, the hackers can steal only encrypted data. They still need your “master password” to decrypt your password file. That master password is the one unique, complex password that you do need to memorize.

WHY YOU NEED A PASSWORD MANAGER

1. It's a place to keep logons, websites, account numbers and passwords all in one place. I use 1Password and it will generate and store strong passwords for me (so I don't have to make them up).
2. It will also let me know if my passwords are weak and recommend that I change them. It tells me how many different websites I'm using the same password for (it's not recommended that you use the same password for everything).
3. It also lets me know if there are any reported security breaches for any of the websites it holds passwords for and recommend that you change them.
4. It will hold all my credit card information, secure notes about anything I want and personal information like my driver's license, passport, etc.
5. Finally, it's part of my estate plan. If something happens to me, there's one place that other family members can go to find all pertinent information; everything from credentials to pay the water bill

to PDFs of my actual estate plan documents. In 1Password, this feature is called the [Emergency Kit](#), which is a fancy name for a mix of computer and handwritten information that you complete and store somewhere secure, like a safety deposit box, that family members can access if needed. It will have confidential access information, so it's not something to keep out in the open.

SECURITY NOTE

[LastPass](#) suffered a [breach](#) in August 2022. The usernames and passwords in the stolen data were encrypted, so a good master password should protect them. Still, given the details in the *Ars Technica* article, replace LastPass with [Bitwarden](#) when comparison shopping.

If online password storage unnerves you, the open-source [KeePass](#) stores password data only locally on your machine, not in anyone's cloud, but that makes you responsible for backing up and securing your data.

GOOD OPTIONS

Top rated password managers include the following (and I strongly recommend the versions you have to pay for - almost all offer a free version that is missing features):

1PASSWORD - <https://www.1password.com/>

BITWARDEN - <https://bitwarden.com/>

DASHLANE - <https://www.dashlane.com/>

KEEPASS - <https://keepass.info/help/v1/setup.html>

ROBOFORM - <https://www.roboform.com/>

TWO FACTOR AUTHENTICATION

This is also known as 2FA or multi factor authentication

WHAT IS TWO FACTOR AUTHENTICATION?

Here's a good definition.

“Two-factor authentication (2FA), sometimes referred to as *two-step verification* or *dual-factor authentication*, is a security process in which users provide two different authentication factors to verify themselves.”¹

Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.

The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include:

KNOWLEDGE FACTORS

A knowledge factor is something the user knows, such as a password, PIN or shared secret.

POSSESSION FACTORS

Possession factors are something the user has, such as an ID card, security token or a smartphone.

INHERENCE FACTORS (AKA BIOMETRICS)

Biometrics are something the user is, something inherently about him or her. “These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns.”²

DISCOVER WHICH SERVICES USE TWO FACTOR AUTHENTICATION

Visit the [2FA Directory](#) to get an idea of which services you use offer two factor authentication.

A PLACE TO STORE YOUR SECOND FACTORS

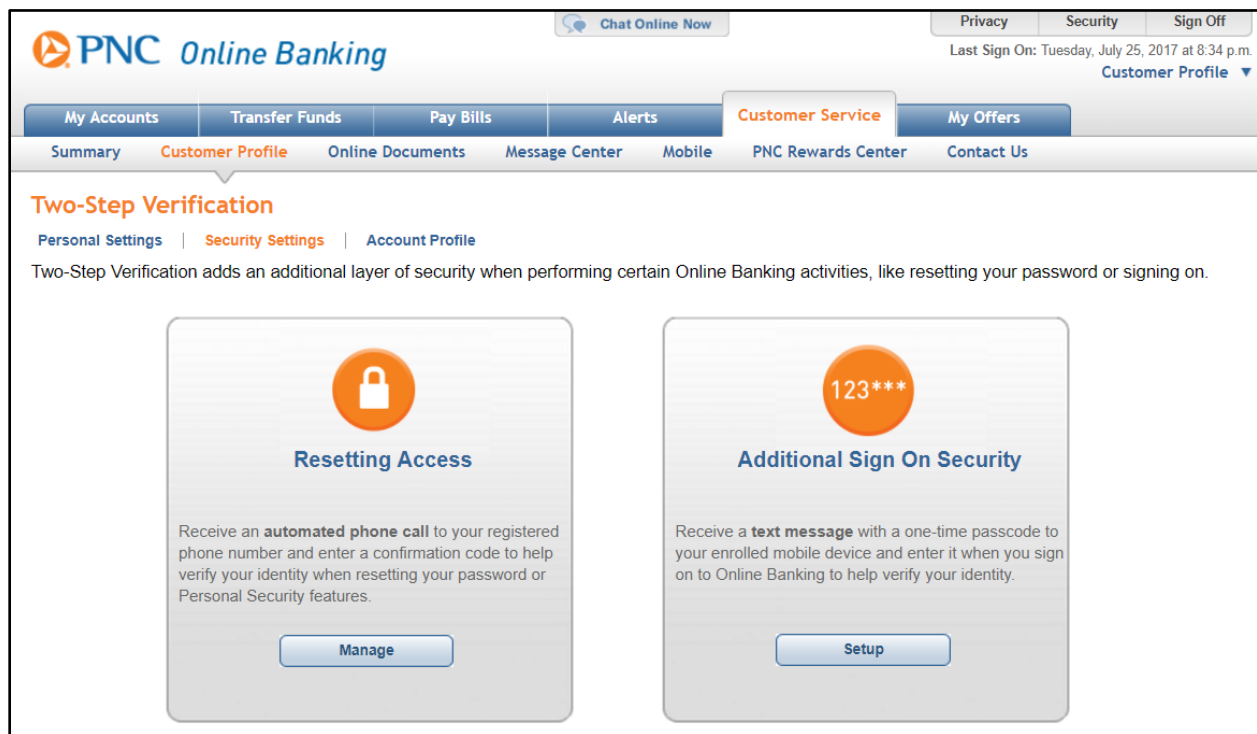
[1Password](#), [Dashlane](#), and [Roboform](#) support storing 2FA codes in their password managers. If you're using another program, you'll need an app like [Google Authenticator](#), [Microsoft Authenticator](#), or [Twilio's Authy](#).

¹ Linda Rosencrance, “Two-Factor Authentication,” TechTarget, accessed March 31, 2023, <http://searchsecurity.techtarget.com/definition/two-factor-authentication>.

² Ibid.

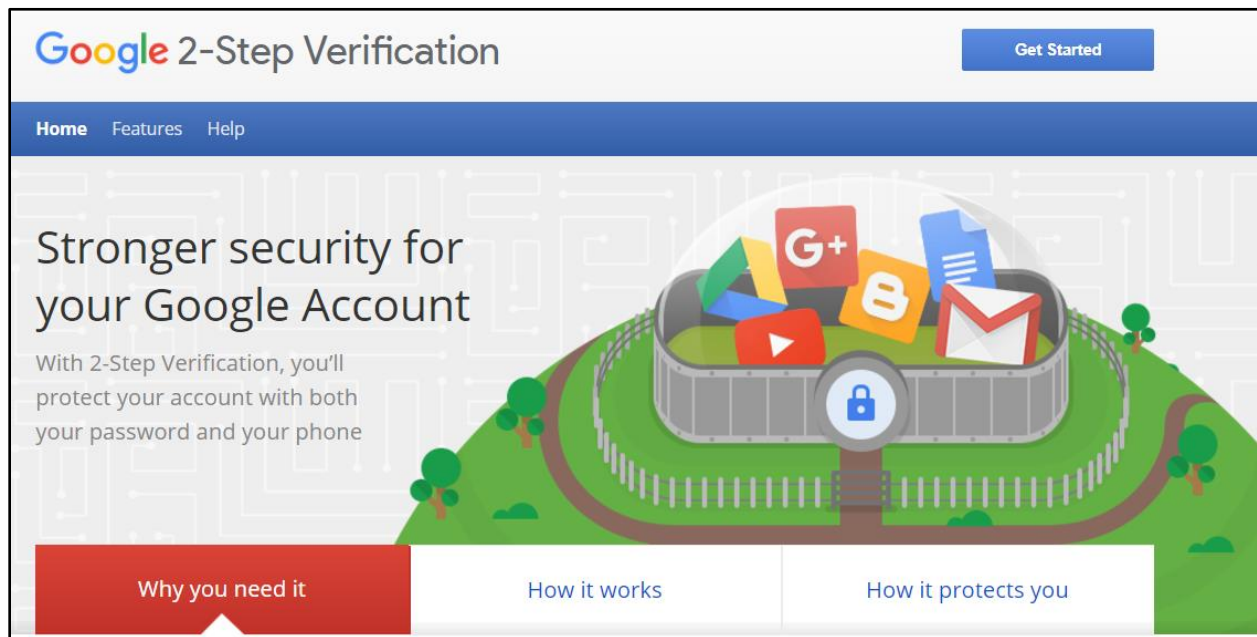
HOW DO YOU GET 2FA?

For critical services you access online, check to see if they offer any type of 2FA. Keep in mind that 2FA is ANNOYING, but better security is almost always more annoying. If you want to protect yourself well, be prepared to be slightly annoyed. Anyway, here are some 2FA ideas. Your bank probably offers it:



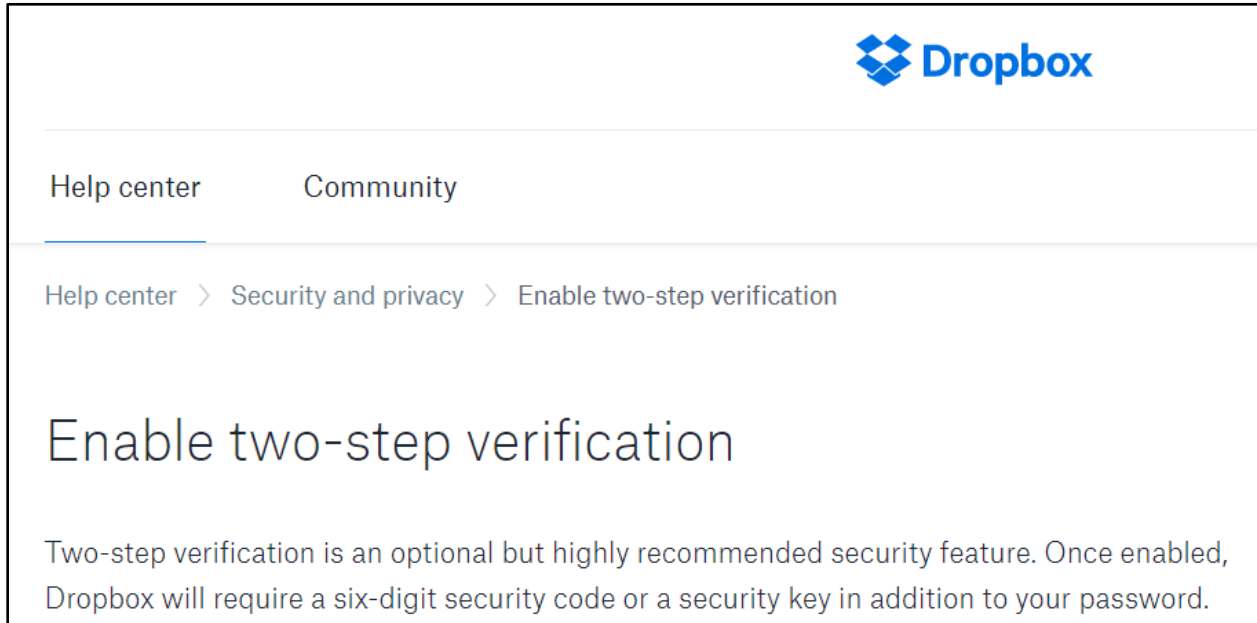
The screenshot shows the PNC Online Banking interface. At the top, there's a navigation bar with links for "My Accounts", "Transfer Funds", "Pay Bills", "Alerts", "Customer Service", and "My Offers". Below this is a secondary navigation bar with "Summary", "Customer Profile", "Online Documents", "Message Center", "Mobile", "PNC Rewards Center", and "Contact Us". The main content area is titled "Two-Step Verification" and includes links for "Personal Settings", "Security Settings", and "Account Profile". A sub-header states: "Two-Step Verification adds an additional layer of security when performing certain Online Banking activities, like resetting your password or signing on." There are two main cards: "Resetting Access" with a padlock icon and a "Manage" button, and "Additional Sign On Security" with a "123***" icon and a "Setup" button. The "Additional Sign On Security" card also includes a description: "Receive a text message with a one-time passcode to your enrolled mobile device and enter it when you sign on to Online Banking to help verify your identity."

Your email account probably offers it:



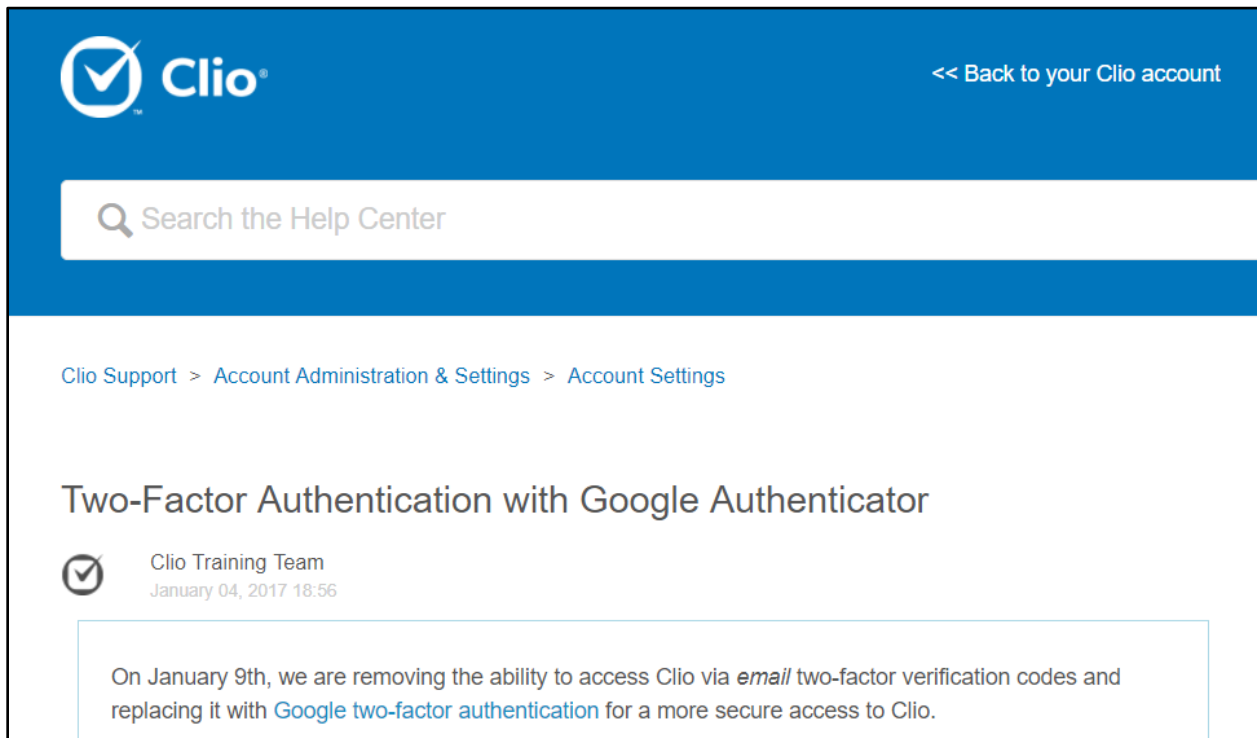
The screenshot shows the Google 2-Step Verification landing page. At the top, it says "Google 2-Step Verification" with a "Get Started" button. Below this is a navigation bar with "Home", "Features", and "Help". The main content area features the heading "Stronger security for your Google Account" and the text: "With 2-Step Verification, you'll protect your account with both your password and your phone". To the right of the text is an illustration of a fenced-in area containing icons for Google+, Blogger, YouTube, and Gmail, with a padlock icon in the foreground. At the bottom, there are three navigation buttons: "Why you need it", "How it works", and "How it protects you".

Your file sharing service probably offers it:



The screenshot shows the Dropbox Help Center interface. At the top right is the Dropbox logo. Below it are two navigation links: 'Help center' (which is underlined) and 'Community'. A breadcrumb trail reads 'Help center > Security and privacy > Enable two-step verification'. The main heading is 'Enable two-step verification'. Below the heading is a paragraph: 'Two-step verification is an optional but highly recommended security feature. Once enabled, Dropbox will require a six-digit security code or a security key in addition to your password.'

Your case management system probably offers it:



The screenshot shows the Clio Help Center interface. At the top left is the Clio logo. At the top right is a link '<< Back to your Clio account'. Below the header is a search bar with the placeholder text 'Search the Help Center'. A breadcrumb trail reads 'Clio Support > Account Administration & Settings > Account Settings'. The main heading is 'Two-Factor Authentication with Google Authenticator'. Below the heading is a post from the 'Clio Training Team' dated 'January 04, 2017 18:56'. The post content is enclosed in a box and reads: 'On January 9th, we are removing the ability to access Clío via *email* two-factor verification codes and replacing it with [Google two-factor authentication](#) for a more secure access to Clío.'

TYPES OF NOTEBOOK COMPUTERS

The categories of notebook computers change regularly and are becoming a bit bewildering. In the last five to ten years, we've seen an explosion of new form factors and use cases, all within the overarching category of "laptop" or "notebook." For our purposes, we will ignore non-business types like "gaming" laptops, but still, a would-be buyer can choose from Ultrabook, Evo, Convertibles, 2-in-1s, and more.

Think back to what laptops looked like and how they behaved about ten years ago. Apart from speed and storage, which would naturally improve over time, they were boxy and ugly. One of the revelations the computer hardware industry learned from Apple's original [MacBook Air](#) was that computers with "enough" power could also be thin, light, and attractive. That original Air is today best remembered for its introduction, where Steve Jobs pulled it out of a standard inter-office mail envelope. Most laptops today, excluding gaming or workstation-class machines, fit in inter-office envelopes. But it was a revolutionary concept then and caused the entire industry to think creatively about form factors.

ULTRABOOKS

[Ultrabook](#) was Intel's first attempt at a coordinated, PC industry-wide response to the MacBook Air. Think ultra-thin, ultra-fast, and ultra-light. Intel defined the initial set of specifications in 2011 and has updated them regularly. An ultrabook is a very thin, light, and powerful notebook PC with excellent battery life, touchscreen capability, and advanced security. Good examples include the [Lenovo ThinkPad X1 series](#) and the [Dell XPS series](#).

ULTRABOOK 2 IN 1 OR CONVERTIBLE

These devices blur the line between a laptop and a tablet and are sometimes called [hybrids](#). The screens detach, flip, or slide into position so that the device is more of a tablet than a laptop. Of these various designs, the "flip" models are more common, affordable, and practical than the "detach" models. Examples of well-regarded "flip" models include Lenovo's [Yoga](#) and [ThinkBook](#) lines. Both have screens that swivel, fold backward, and support pen-based input, similar to many tablets. Their advantage over tablets is that they also run standard Windows applications and possess traditional keyboards and trackpads built-in rather than as add-on accessories.

Additional examples of 2-in-1s include the [Microsoft Surface Pro](#) and the [HP Elite x360 models](#).

Determining if a 2-in-1 fits your practice depends mainly on how mobile you are, *i.e.*, how often you visit client sites, and whether you have found or think there is a place for pen-based input, such as digital notetaking. As mentioned above, the advantage of the "switchable" form factor is that you get a "real computer" and a tablet in one device. The disadvantages include losing some truly attractive tablet features—battery life, portability, and an overall better notetaking experience.

EVO LAPTOPS

Intel's [Evo](#) specification is the successor to Ultrabook. The Evo laptop specifications from Intel require a manufacturer's laptop to support Wi-Fi 6, Thunderbolt 4, and get at least 9 hours of battery life. Evo has not introduced new form factors as Ultrabook did; instead, it focuses primarily on internal improvements. Additionally, the Evo brand hasn't received the same marketing push or notoriety. For research and shopping purposes, you will likely find ads conflating Ultrabook and Evo. In those cases, pay primary attention to the specs rather than the marketing term. For example, Intel's website advertises certain models of the Dell XPS, HP x360, and Lenovo Yoga as Evo laptops.

OTHER CATEGORIES

If you look at reviews of laptops on a site like [Laptop Mag](#) or [Wirecutter](#), they use categories like best Ultrabook, best gaming laptop, best laptop/tablet (see 2-in-1 above), and best business laptop. In our professional opinion, you're better off looking for a business laptop. Some notebook models are aimed at business users, and others are not. Pay attention to the product positioning because it signifies meaningful differences in everything from included software and price to available support and product durability.

VETTING AI FOR ATTORNEYS

By: Morgan Germann, Affinity Consulting Group LLC

INTEGRATING AI INTO YOUR LAW FIRM? CONSIDER THESE FIRST

Whether you realize it or not, artificial intelligence (AI) is already an integral part of our daily lives. Video games, voice assistants, and online recommendation algorithms have all used AI for years. So, why is everyone [talking about it now](#)? Why, [ChatGPT](#), of course.

OpenAI released its innovative chatbot, ChatGPT, in December 2022. Its arrival generated significant enthusiasm about the potential of generative AI. Generative AI is an artificial intelligence that can autonomously generate new content, such as text passages, images, or even music. It finds patterns and examples in existing data and uses that to create something new based on a prompt from the user. When you ask a program like ChatGPT a question, it won't just scrape a response from the internet, but will look at every existing response in its database and synthesize them to create its own unique response.

While no one knows for certain what the future holds for this groundbreaking technology, lawyers are already asking themselves how they can start harnessing the power of generative AI to enhance their legal practice. But, with so many new tools and services popping up daily, it can be challenging to figure out which is right for you. To that end, you should consider several factors when analyzing which tools to integrate into your law firm.

YOUR GOAL

To embark on the most efficient journey, you must have a clear destination in mind. Therefore, define your goals before you begin exploring AI tools. With its ability to analyze, summarize, and compare information, generative AI has the potential to do in seconds what would take you all night to do manually. While many AI tools are still undergoing beta testing, understanding AI's current strengths and capabilities will provide valuable insights into how it can help your firm today and in the future. Here are some of the tasks that AI is currently being designed to help you accomplish:

LEGAL RESEARCH

Research can be difficult and tedious, costing your practice both time and money. AI-powered research tools can automate the process of searching through legal databases and quickly retrieving relevant cases, statutes, regulations, and legal opinions.

DATA ANALYSIS

Instead of spending time pouring over historical legal data to create predictive analytics, forecast case outcomes, estimate settlement values, or identify potential litigation risks, let an AI-powered tool summarize the data for you.

DATA VISUALIZATION

Communicating large and complex data sets can be difficult, especially if your audience isn't well-versed in the topic you're attempting to convey. Generative AI can help make visuals that will not only explain vast datasets to other people, but to you as well.

CONTRACT ANALYSIS AND REVIEW

While it's essential to review every contract carefully, having a tool that can quickly create summaries and highlight key terms, obligations, and provisions helps you understand a contract even before you begin reading. AI can also compare clauses across multiple contracts, ensure compliance with industry standards, search for potential

inconsistencies and risks, and highlight possible issues to direct your attention to noteworthy points in an individual contract.

DUE DILIGENCE AND EDISCOVERY

While crucial to your job, these tasks can drain your limited resources, and outsourced human-based eDiscovery may prove too slow or costly. Generative AI models can help analyze and review large volumes of documents and other relevant materials and flag critical information, potential risks, and anomalies. It can also classify and categorize documents based on specific criteria and go through the material to redact sensitive or privileged information.

WRITING

Generative AI can help you draft and edit papers, ensuring you produce the best possible documents. It can analyze what you've written and provide suggestions, proofread, check your grammar, and even suggest a structure for your legal arguments.

CLIENT COMMUNICATIONS

AI models can help categorize and prioritize client emails, ensuring that urgent matters receive prompt responses. You can also integrate an AI-powered chatbot into your website to provide your clients with 24/7 support to answer their questions and guide them through basic processes.

TRANSLATING LEGALESE

Instead of reviewing a document point-by-point and explaining everything to your client, generative AI can help rephrase complicated wording and summarize passages in a simple and accessible fashion. The law may require complex phrasing, such as in the tax code, but AI may save you explanatory time with clients.

FINDING “YOUR AI”

With so many new products based on generative AI appearing in the market, each vying to find their niche, focus on what exactly you want to accomplish. This provides a strong starting point so you know what to type into your search engine to find the perfect product for your practice.

THE AI'S AUDIENCE

AI tools are becoming increasingly diverse, catering to various tasks and audiences. Some tools, like Google's [Bard](#), offer general assistance, including translating languages and answering everyday queries. Others, like [Casetext](#), are explicitly designed to support lawyers with specialized tasks, such as legal research. When searching for the best AI tool for your firm, consider its intended function and its target audience.

Aligning your goals with the right AI tool requires careful consideration beyond just shared objectives. It's important to recognize that an AI tool might be suited for a different audience, even if it aligns with your specific goal. For instance, if you open your search engine and look for an AI that analyzes data, you might find [Tableau](#). While this tool may help business executives create reports, it may not be so good with predictive legal analytics. When considering AI tools to reach your objectives, begin with products designed for the legal market.

The legal field is full of unique requirements and challenges when finding a helpful AI tool. Since law is a location-based practice, permissions and restrictions vary by state, province, and country. Confirm that the AI tool was trained for your jurisdiction. [Amto](#) is an AI tool that aims to help lawyers draft letters, contracts, briefs, blogs, and emails. However, since it was trained on Indian laws and regulations, it may be unable to perform all these tasks for lawyers outside India effectively. Find an AI tool trained on the relevant information for your jurisdiction.

ACCURACY

If you've ever taken a math class, your teacher has asked you to show your work and provide evidence for your answer. This is something that AI struggles to do. For example, if you ask ChatGPT for the reasoning behind its answer, it says that it synthesizes information from multiple sources in its database to formulate responses. Because

it uses its entire training dataset to grasp grammar, syntax, and context rather than exclusively relying on sources directly related to the question at hand, it cannot attribute its answer to a specific list of sources.

This problem is closely linked to another challenge commonly observed in generative AI, particularly when you use it to conduct research. When AI generates human-like text, it uses its accumulated knowledge to guess the next word based on the preceding context. This may produce responses that sound plausible but are entirely fictitious. Developers commonly refer to these responses as “hallucinations.”

This problem is especially prevalent when ChatGPT is asked to perform literature reviews for researchers. It’s not uncommon for ChatGPT to reference nonexistent papers, falsely attributing them to field experts and claiming that they were published in reputable journals. This is just one example of a context where generative AI creates its own facts by analyzing historical patterns. While this system works very well to generate natural-sounding speech, this is a terrible way to conduct research.

It’s not only issues with the program itself that can lead to inaccurate answers, but also flaws within its dataset. These issues manifest in various ways. For example, outdated information can lead AI to generate inaccurate responses. Because ChatGPT relies on a database compiled in 2021, it has limited-to-no knowledge of anything that happened after that point. In an evolving field like law, this presents a problem. For example, if you were to ask ChatGPT about abortion access in the United States of America, it would be unaware of the obvious relevance of the *Dobbs v. Jackson Women’s Health Organization* decision. This is why it’s important to double-check any information that generative AI gives you.

CONFIDENTIALITY

Preserving clients’ confidentiality is one of the most essential obligations attorneys have. Therefore, you must carefully review and comprehend the terms of service associated with any generative AI platform you plan to use. A clear understanding of how it handles the information you provide is essential to ensure that confidential information remains solely between you and your client. Check if the AI platform will use the information you supply to train its system. If so, you must be careful not to violate your client’s confidentiality.

Because confidentiality is so critical, many AI programs designed for lawyers take extra precautions to protect your client’s information. [Harvey](#), for example, is an AI platform made to help lawyers with data analysis, due diligence, litigation, and regulatory compliance that has recently partnered with the London-based law firm Allen & Overy and aims to create AI systems for law firms that are “not only powerful, but also scalable, transparent, and secure.” Even with promises of increased privacy, remember that you are interacting with a third-party entity. Therefore, exercise caution and refrain from sharing any information that a third party should not be able to access.

COST AND AVAILABILITY

Some AI tools, such as ChatGPT, are free and widely available. Other tools like [Westlaw](#) are expensive and only available to a limited audience of beta testers. This is especially true of programs designed specifically for lawyers that contain updated information and increased security measures.

Determining whether it’s worth it to pay a premium and sit around on a waiting list at this stage in AI’s evolution circles back to your goal for the AI system. If you are looking to use it to help draft and edit documents or hoping for help translating and summarizing confusing language for clients, then there may be no reason to pay when ChatGPT is free. However, if you need an AI platform that can handle sensitive information, contains up-to-date legal information, or can handle a specialized task such as reviewing a contract, then it may be worthwhile to pay for a more expensive program not generally available to the public.

From legal research to data analysis, AI can help remove some of the tedium from your job, allowing you to work faster and complete tasks more efficiently. However, you must exercise caution when deciding what AI platform to use by carefully considering your goal as well as the platform’s audience, accuracy, confidentiality, cost, and availability. Because of law’s sensitive and ever-changing nature, don’t rely entirely on this burgeoning technology.

Instead, exercise prudence by verifying and cross-checking AI's output, especially when it can't clearly explain how it generated its answer.

VIRTUAL REALITY, AUGMENTED REALITY, AND ARTIFICIAL INTELLIGENCE IN A REAL LAW FIRM

By: [Zachary T. Glaser, Esq.](#), legal tech advisor at Affinity Consulting Group LLC

Virtual Reality (VR), Augmented Reality (AR), and Artificial Intelligence (AI) are more accessible than ever. Their increasing commercial viability will fuel that trend into the foreseeable future. Clients, courts, businesses, opposing counsel, and the rest of the world are embracing both the benefits and the detriments of these technologies. Like it or not, lawyers and law firms need to understand them.

But what are VR, AR, and AI, other than LinkedIn buzzwords, and how should law firms use them? The short answer: they are tools. And unless one employs them to make the firm's life easier, they are just shiny objects that tend toward distraction, at best, and censure for the lazy, at worst.

These tools, though, can increase a firm's efficiency, productivity, and accuracy by orders of magnitude. Firms can advise their clients better, assist them more quickly, or even provide services previously unavailable or financially unfeasible.

Let's take a basic look at these three emerging trends and see what they are, how they are currently used, and what pitfalls we may need to watch out for.

VIRTUAL REALITY

Virtual Reality, according to *The WIRED Guide to Virtual Reality* is, "a technology by which computer-aided stimuli create the immersive illusion of being somewhere else..."¹ Frankly, that is about as good a definition as anything else. These immersive experiences can come in the form of special rooms with large screens (i.e., flight simulators), or the more common head-mounted displays of VR headsets.² They can incorporate audio stimuli, body and eye movement tracking, and even haptic feedback.³ Some of the more advanced VR gaming systems even use a treadmill to simulate walking or running in the virtual world.⁴

The key factor, however, is the illusion of being somewhere else, no matter the depth of the experience. VR attempts to take a user to another location altogether. It can be used in evidentiary proceedings to provide a reasonable representation of actions, locations, or specific scenarios. Or it can be a place where clients meet with your firm, avatar-face to avatar-face.

¹ Rubin, P., & Grey, J. (2020b, March 8). What is Virtual Reality (VR)? The Complete WIRED Guide. WIRED. <https://www.wired.com/story/wired-guide-to-virtual-reality/>.

² Wikipedia contributors. (2001, October 3). *Virtual reality*. Wikipedia. https://en.wikipedia.org/wiki/Virtual_reality.

³ Id.

⁴ Fisher, T. (2021, February 28). What is virtual reality? Lifewire. <https://www.lifewire.com/virtual-reality-vr-definition-4155090>.

AUGMENTED REALITY

Augmented Reality, on the other hand, is not immersive. It is additive or destructive, depending on the goals. It combines real-world and computer-generated content to enhance a user's perception of the physical space around them.⁵ Instead of creating a virtual environment out of whole cloth, AR systems must map and track a physical environment while simultaneously displaying and tracking a companion virtual environment. It is not enough to simply display something to a viewer (i.e., running pace, or other information from a smart watch). The virtual environment must be incorporated into the user's perception of the physical world (i.e., ghost pacer leading a runner through their route).

AR requires the ingestion of data that many people would consider personal or private. An app that shows a user what a specific couch would look like in their living room will need a lot of information about the user's house. Even a product as simple as a filter that places a bird on a user's shoulder will have to gather information about its subject.

ARTIFICIAL INTELLIGENCE

Artificial Intelligence is the most complex of these three technologies. It is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.⁶ AI use-cases and technologies vary from software that can defeat the world's best chess players⁷ to predictive text in iMessages.⁸ One can even use AI to create remarkable headshots with products like Fotor, and Aragon.ai. Mostly, though, AI is used for much less glamorous tasks like background noise reduction or detecting fraudulent transactions.

For now, at least, these tools need to be built for purpose. So-called Artificial General Intelligence (AGI) is still hypothetical.⁹ Although ChatGPT seems to know everything, it most certainly does not. And when attorneys use AI tools for purposes beyond their capabilities, they can get into trouble.¹⁰

This is because, at its core, the output of Artificial Intelligence is simply based on probabilities. Which can be good or bad, depending on the purpose. If doctors use AI to flag items for review, it can increase efficacy. If courts use AI to determine potential for recidivism, it can magnify bias¹¹.

However, to get these probabilities to something even remotely helpful, AI tools need to process a fantastic amount of data. If a judge has only ruled twice on a particular issue, even a well-trained AI tool will be hard pressed to predict the outcome of a third case with any accuracy. On the other hand,

⁵ Wikipedia contributors. (2024, January 2). Augmented reality. Wikipedia. https://en.wikipedia.org/wiki/Augmented_reality

⁶ Copeland, B. (2024, January 4). Artificial intelligence (AI) | Definition, Examples, Types, Applications, Companies, & Facts. Encyclopedia Britannica. <https://www.britannica.com/technology/artificial-intelligence>

⁷ Wikipedia contributors. (2024a, January 1). Deep Blue versus Garry Kasparov. Wikipedia. https://en.wikipedia.org/wiki/Deep_Blue_versus_Garry_Kasparov

⁸ Johnson, K. (2023, September 13). The iPhone 15 opts for intuitive AI, not generative AI. WIRED. <https://www.wired.com/story/apple-iphone-15-opts-for-intuitive-ai-not-generative-ai/>

⁹ https://en.wikipedia.org/wiki/Artificial_general_intelligence

¹⁰ Patrice, J., (2023, May 30). For the love of all that is holy, stop blaming ChatGPT for this bad brief. Above the Law. <https://abovethelaw.com/2023/05/chatgpt-bad-lawyering/>

¹¹ Fry, H. (2018). *Hello World: Being Human in the Age of Algorithms*. W.W Norton & Company, Inc.

with decades of feedback from ReCAPTCHA users, Google has trained AI to digitize millions of books and print articles.¹²

Even built-for-purpose AI has its problems, though, especially when users rely on it to make a specific decision. When outcomes are based on massive amounts of data and years of feedback, it is hard to articulate how the tool came to that decision. This can make it next to impossible to check its accuracy. As such, regulators increasingly focus on these so-called black boxes and a user's ability to explain why a tool came to a particular decision.¹³

Since AI models require unprecedented amounts of data, these tools are often trained on information protected by copyright. Commonly, they "create" output that looks remarkably similar to the products they are trained on. A Fair Use war is already being waged in the courts by writers, visual artists, musicians, stock photo providers, and other publishers against the likes of OpenAI and Meta.¹⁴

Users should know how the AI tool works, even if it's built-for-purpose. For lawyers and law firms, the specific danger is confidentiality and privilege. If a lawyer trains an AI tool on client data, they must confirm the data does not make its way into a third-party's hands. This includes information provided via a chatbot's prompt and any files the lawyer loads into the tool.

A law firm should not avoid AI outright, though. There are plenty of tasks that have built-for-purpose tools waiting to increase a firm's efficiency or accuracy. And, as firms look to direct the power of AI to their own data, the above concerns can be mitigated and avoided through careful consideration. Providers like NetDocuments and CoCounsel have already addressed these concerns with some of their tools. And the firm's IT department should be able to ask the right questions—provided they are considering the appropriate dangers.

IMPLEMENTING AR, VR, AND AI IN A FIRM

Ultimately, AR, VR, and AI are simply tools a law firm can use to assist their broader purpose of serving clients. It's easy to look at these technologies and create purposes for them in the office, which can easily create more work for the firm. As with all technology implementation, the challenge is using these tools to enhance existing processes. Remember, if your office doesn't need Virtual Reality, it would be ill-advised to buy headsets for all the associates. It may be fun, but it probably won't increase productivity, or lead to more billable hours.

¹² O'Malley, J. (2018, January 12). Captcha if you can: how you've been training AI for years without realizing it. TechRadar. <https://www.techradar.com/news/captcha-if-you-can-how-youve-been-training-ai-for-years-without-realising-it>

¹³ Consumer Financial Protection Bureau. (2022, May 26), *Adverse action notification requirements in connection with credit decisions based on complex algorithms*. https://files.consumerfinance.gov/f/documents/cfpb_2022-03_circular_2022-05.pdf

¹⁴ Appel, G. (2023, April 11). Generative AI has an intellectual property problem. Harvard Business Review. <https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem>

WIRELESS ENCRYPTION

ROBUST AND SECURE WI-FI

It's hard to believe Wi-Fi has existed for over 20 years. We all learned the value of reliable in-home internet over the last couple of years. Perhaps you found that what satisfied the "Netflix need" didn't satisfy work-from-home. Two new technologies are here to make home Wi-Fi better.

The first is "mesh networking." Traditionally, you had a single wireless signal from one point in your home, usually next to, or even built into, your router. The further you got from that point, the slower or less reliable your connection became until it dropped entirely. Mesh networks replace that single broadcast point with multiple points, which seamlessly blanket your house with a single Wi-Fi network. These systems are sold in two and three packs and come with software to help you place each relay box, called a "node," at the right spot in your house.

The second feature is "Wi-Fi 6", the sixth generation of wireless networking. Wi-Fi 6 is up to 250% faster than your existing wireless setup, supports 50+ simultaneous device connections, which is great for small and mid-sized firms, and enables the latest wireless connection security, known as WPA3. I recently installed a mesh Wi-Fi 6 system in my home, the [eero 6 ProE](#) and have been very happy with it.

HOME OR WORK WIRELESS CONNECTIONS

If you rely on a wireless Internet connection at your office or home to work with sensitive client information, your wireless router or access point must be properly encrypted. If you set it up yourself and aren't sure, then you should immediately secure expert assistance to ensure that your security is properly configured. Sometimes, it's as easy as calling the technical support line for the manufacturer of your router. The big companies that sell wireless routers all have technical support representatives that can walk you through the process over the phone. In case you're wondering, big names in wireless routers include [D-Link](#), [eero](#), [Synology](#), and [TP-Link](#).

RISK OF USING PUBLIC WI-FI

First, you need to be educated about this subject. For a quick primer, here are two short articles that will bring this issue into focus: [Here's what an eavesdropper sees when you use an unsecured Wi-Fi hotspot](#) by Eric Geier and [What Are Packet Sniffers and How Do They Work?](#) by Andy O'Donnell. For an interesting discussion of this in the legal arena, see the now famous California Formal Opinion No. 2010-179 which states:

"With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, **Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.** Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so."¹

¹ See <https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/2010-179-Interim-No-08-0002-PAW.pdf>, emphasis added.

HOW TO PROTECT YOURSELF

CELLPHONE WI-FI HOTSPOT

Rather than connecting to the public Wi-Fi wherever you are, consider using a cellular hotspot or MiFi. Properly configured, these connections are a secure way to connect your notebook or tablet to the Internet via the phone hotspot.

CONSUMER VPN SERVICES

There are many services that allow you to create a Virtual Private Network connection even though you're using a public and otherwise unsecured Wi-Fi connection. "In the simplest terms, a VPN creates a secure, encrypted connection between your computer and the VPN's server. This tunnel makes you part of the company's network as if you are physically sitting in the office, hence the name. While connected to the VPN, all your network traffic passes through this protected tunnel, and no one in between can see what you are up to. A consumer VPN service does the same thing but extends that protection to the public."² Here are some options for this:

- [CyberGhost](#);
- [Encrypt.me](#);
- [ExpressVPN](#);
- [IPVanish](#);
- [NordVPN](#);
- [Private Internet Access](#);
- [ProtonVPN](#);
- [SurfShark](#); and
- [TunnelBear](#).

FIREWALL

WHAT IS A FIREWALL?

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be hardware, software, or a combination of both.³ For laptops and desktops, both macOS and Windows 11 have firewalls built-in, as have several prior editions of each software. However, these firewalls don't easily provide details on what they're doing. If you want more visibility into your network traffic, look at [Little Snitch](#) for Mac and [GlassWire](#) for Windows.

YOUR OBLIGATION

You need to ensure that a firewall is in place at your office and anywhere you use your computer and connect to the Internet. You can test yourself using services like [ShieldsUP!](#). If you aren't sure if you are being protected, then you should contact a security expert to conduct a penetration test. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.⁴

² *The Best VPN Services for 2024*, Chris Stobing, July 29, 2024, PCMag, <https://www.pcmag.com/picks/the-best-vpn-services>.

³ See <http://www.webopedia.com/TERM/F/firewall.html>.

⁴ See https://en.wikipedia.org/wiki/Penetration_test