William Smith
8th Annual Technology & Justice for All CLE

USING AND SECURING TECH SYSTEMS FOR LAWYERS

Basic information security overview for Texas lawyers

DIRECT ETHICAL DUTY

TEXAS DISCIPLINARY RULES OF PROFESSIONAL CONDUCT

(Including Amendments Effective May 1, 2018, June 1, 2018 and February 26, 2019)

Rule 1.01. Competent and Diligent Representation

(a) A lawyer shall not accept or continue employment in a legal matter which the lawyer knows or should know is beyond the lawyer's competence, unless:

(1) another lawyer who is competent to handle the matter is, with the prior informed consent of the client, associated in the matter; or

(2) the advice or assistance of the lawyer is reasonably required in an emergency and the lawyer limits the advice and assistance to that which is reasonably necessary in the circumstances.

(b) In representing a client, a lawyer shall not:

(1) neglect a legal matter entrusted to the lawyer; or

(2) frequently fail to carry out completely the obligations that the lawyer owes to a client or clients.

(c) As used in this Rule, "neglect" signifies inattentiveness involving a conscious disregard for the responsibilities owed to a client or clients.

Maintaining Competence

8. Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology. To maintain the requisite knowledge and skill of a competent practitioner, a lawyer should engage in continuing study and education. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances. Isolated instances of faulty conduct or decision should be identified for purposes of additional study or instruction.

IMPLIED ETHICAL DUTY

Rule 1.05. Confidentiality of Information

(a) "Confidential information" includes both "privileged information" and "unprivileged client information." "Privileged information" refers to the information of a client protected by the lawyer-client privilege of Rule 503 of the Texas Rules of Evidence or of Rule 503 of the Texas Rules of Criminal Evidence or by the principles of attorney-client privilege governed by Rule 501 of the Federal Rules of Evidence for United States Courts and Magistrates. "Unprivileged client information" means all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client.

(b) Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e) and (f), a lawyer shall not knowingly:

(1) Reveal confidential information of a client or a former client to:

(i) a person that the client has instructed is not to receive the information; or

(ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm.

(2) Use confidential information of a client to the disadvantage of the client unless the client consents after consultation.

(3) Use confidential information of a former client to the disadvantage of the former client after the representation is concluded unless the former client consents after consultation or the confidential information has become generally known.

(4) Use privileged information of a client for the advantage of the lawyer or of a third person, unless the client consents after consultation.

(c) A lawyer may reveal confidential information:

EVERYTHING I DO IS THROUGH TECH, HOW DO I GET MY ARMS AROUND THIS??

Cybersecurity frameworks

- Provide a structured approach to evaluating, implementing, and maintaining information security practices
- ISO 27001 Controls (Annex A)
- HIPAA Security Rule
- NISTIR 7621 Small Business Information Security
- PCI DSS

HIPAA SECURITY RULE

- **Security standards: General Rules** - includes the general requirements all covered entities must meet; establishes flexibility of approach; identifies standards and implementation specifications (both required and addressable); outlines decisions a covered entity must make regarding addressable implementation specifications; and requires maintenance of security measures to continue reasonable and appropriate protection of electronic protected health information.
- **Administrative Safeguards -** are defined in the Security Rule as the "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."
- **Physical Safeguards -** are defined as the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
- **Technical Safeguards -** are defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."
- **Organizational Requirements -** includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans.
- **Policies and Procedures and Documentation Requirements** - requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the Security Rule; maintenance of written (which may be electronic) documentation and/or records that includes policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.

NIST SMALL BUSINESS INFORMATION SECURITY

NIST SMALL BUSINESS INFORMATION SECURITY

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

  Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

  The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

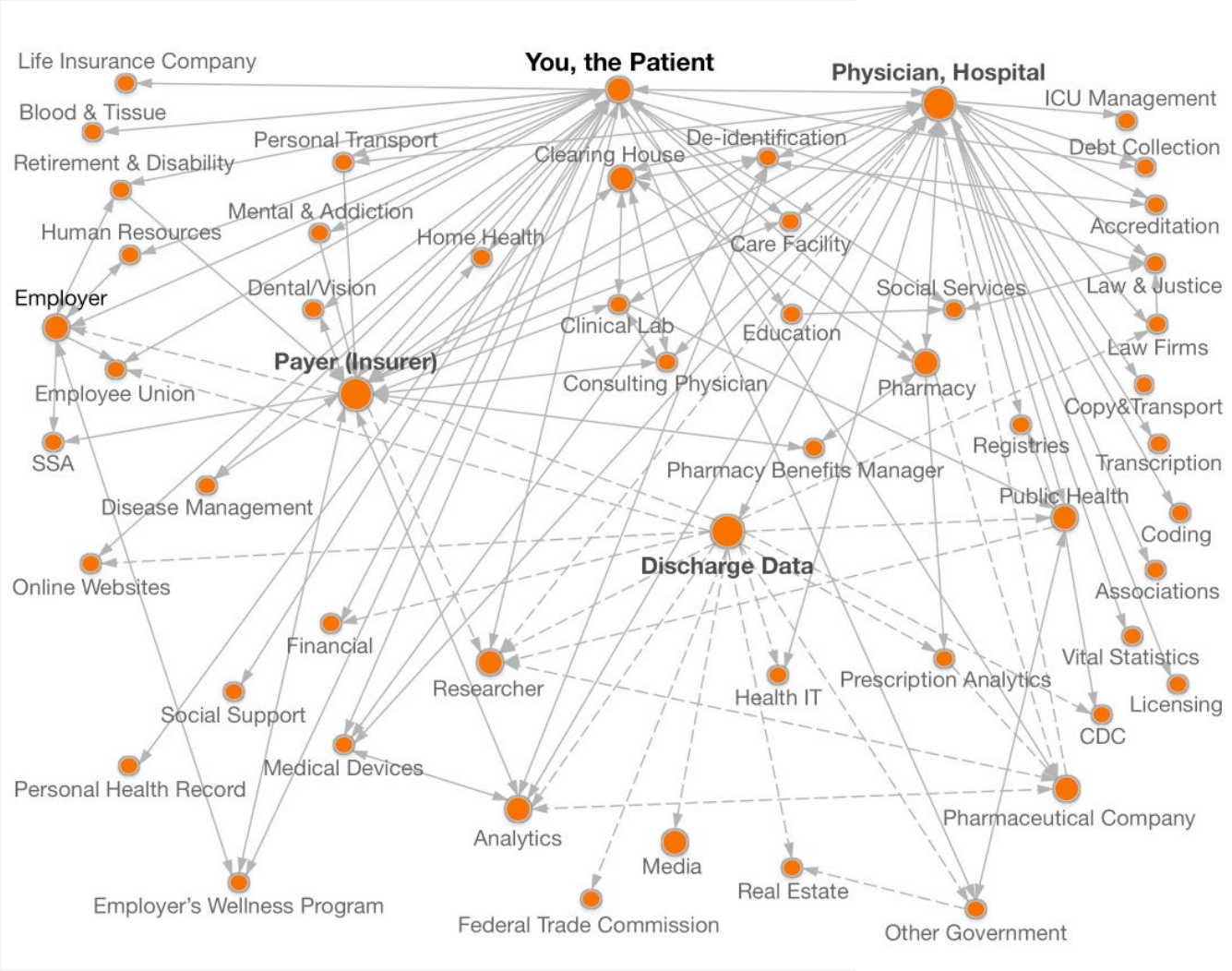
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

  The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

DUDE, WHERE'S MY DATA?

Create a data map

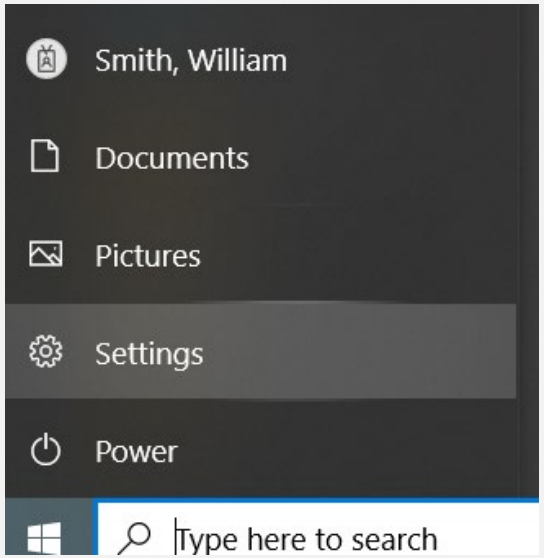
- You can't figure out how to protect your information until you know where it is
- Spend 30 minutes writing down all of the places where client or firm information is stored or processed
- "Mindmaps" can be a useful tool for this (Google it)
- Can be helpful to think about a particular document, and the path it took to get from inception to where you are looking at it
  - E.g.: new client intake form: Emailed to Client (MS Exchange) a link to a web form (Google forms) which generates a PDF that I store on my computer (local device) in a folder that is mirrored on the cloud (Dropbox)
- Or think about a business process, and the technology required to complete it



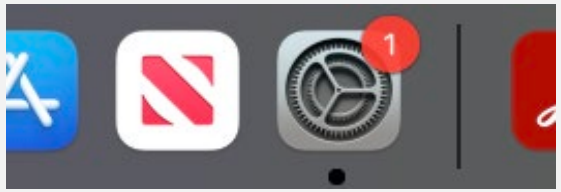
https://thedatamap.org/

SECURING DEVICES

Windows

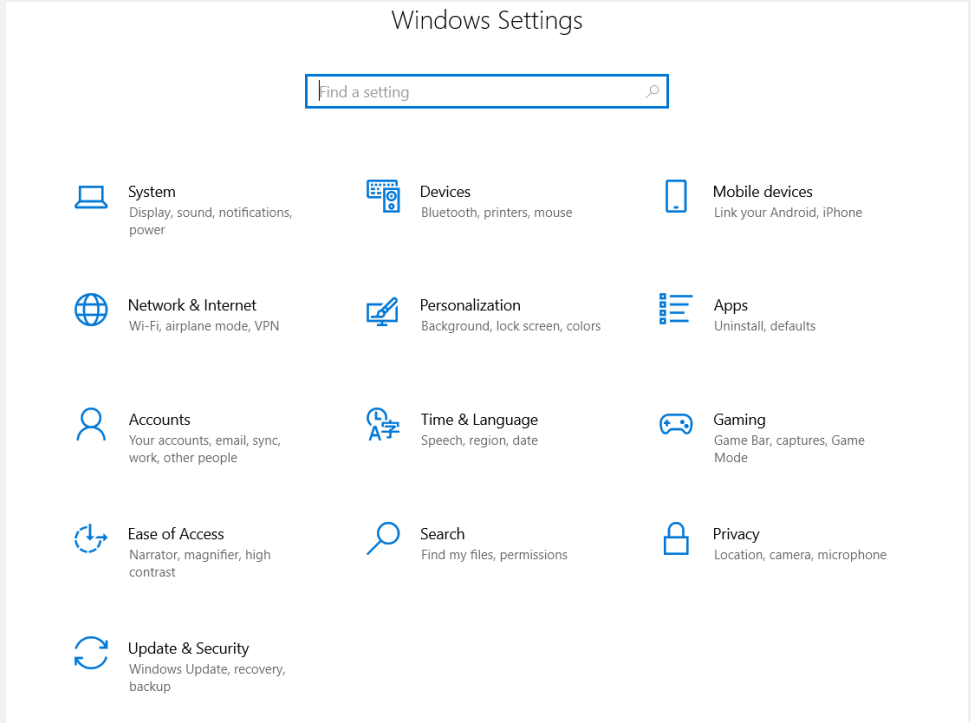


Mac

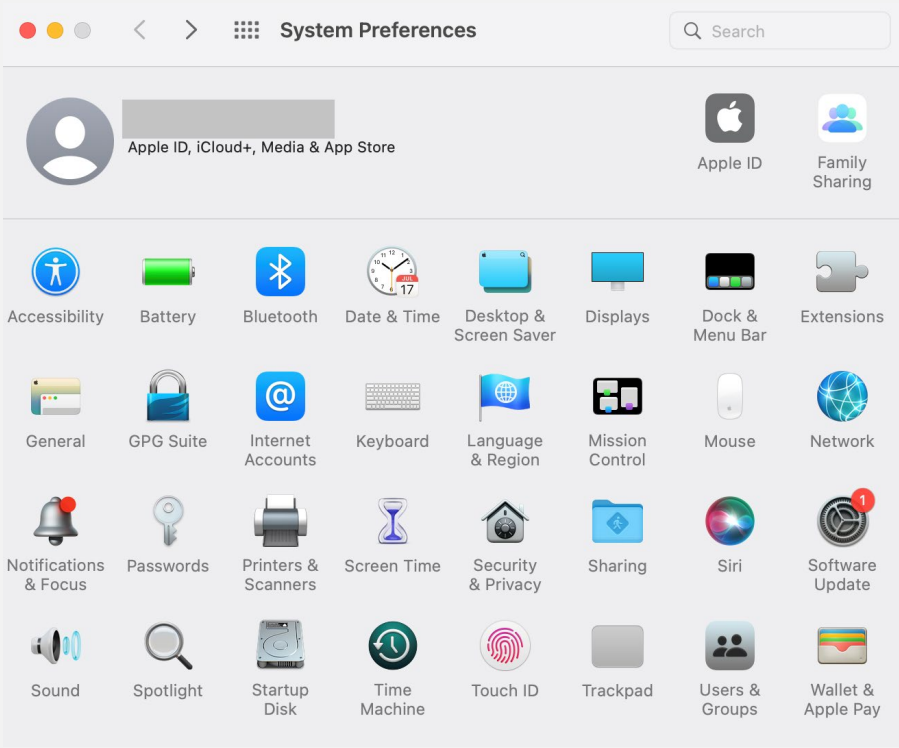


SECURING DEVICES

Windows



Mac

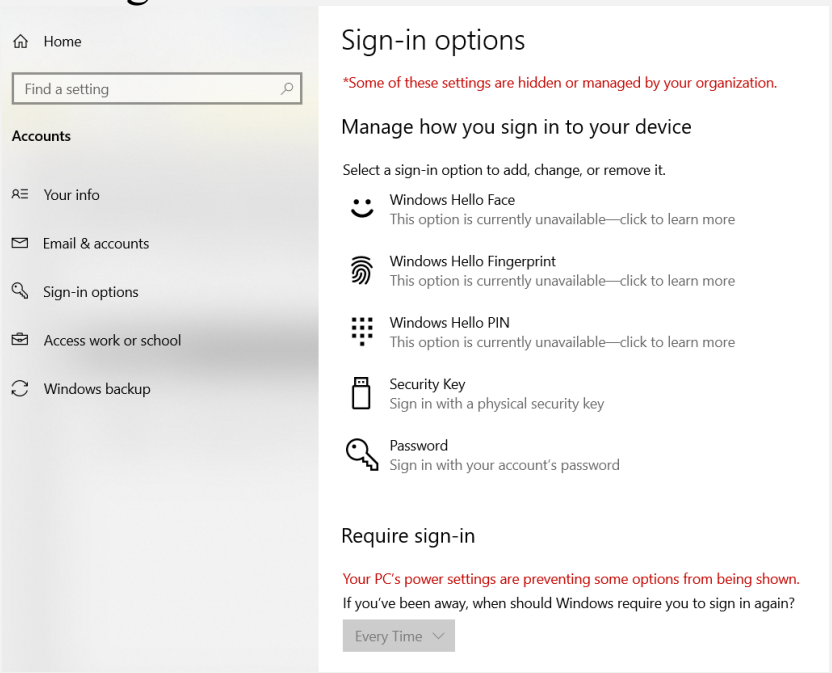


SECURING DEVICES

1. Set a system password and an automatic screen lock

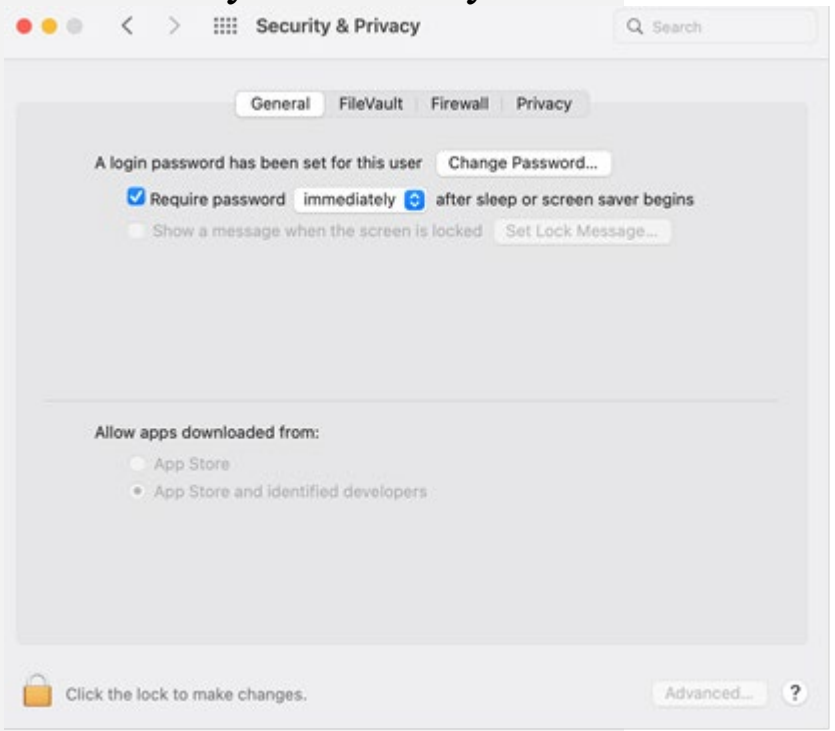
Windows

- Settings > Accounts > Sign-in Options
- Settings > Personalization > Lock Screen



Mac

- System Preferences > Security and Privacy > General

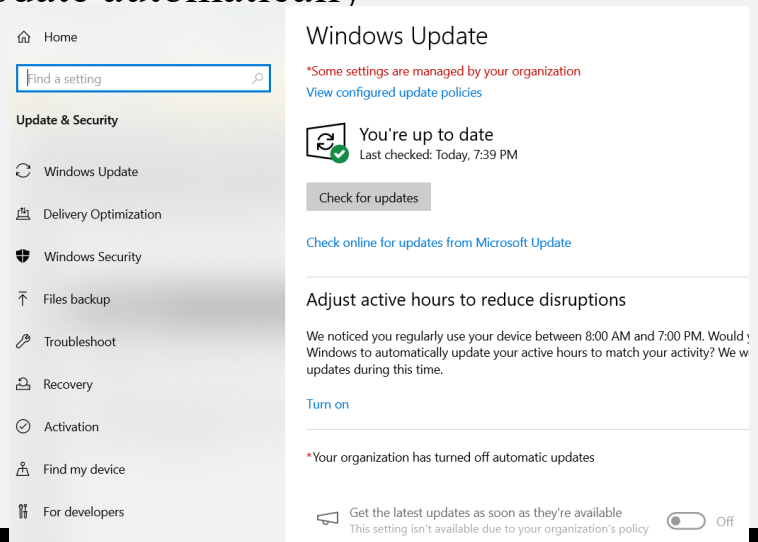


SECURING DEVICES

2. Enable automatic OS updates

Windows

- Settings > Update & Security > Windows Update
- Configure other frequently used software such as MS Office and Google Chrome to update automatically



Mac

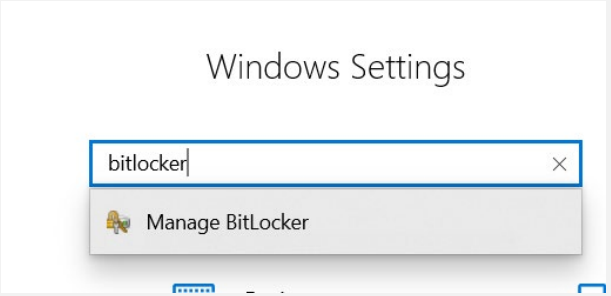
- System Preferences > Software Update
- Configure other frequently used software such as MS Office and Google Chrome to update automatically

SECURING DEVICES

3. Enable local disk encryption

Windows

- Settings > Type “Bitlocker” into Settings search bar > Manage Bitlocker
- Make sure you back up your recovery key!
- Consider using a sticker with contact info



Mac

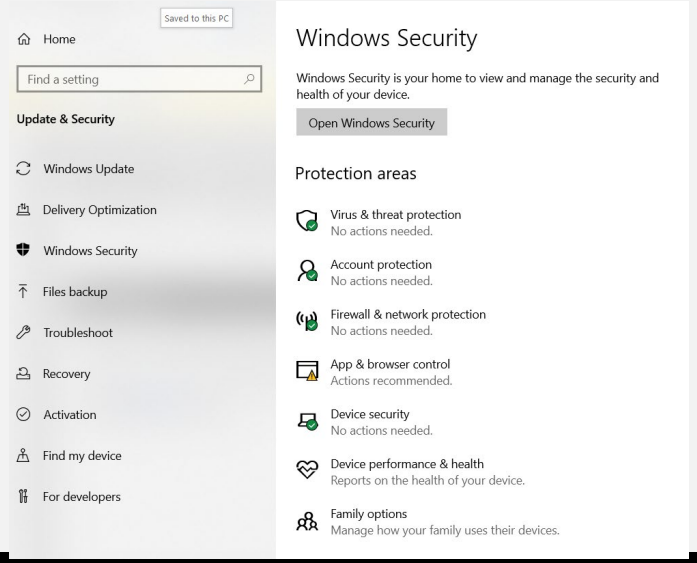
- System Preferences > Security and Privacy > FileVault
- Make sure you back up your recovery key!
- Consider enabling a lock screen message: System Preferences > Security and Privacy > General > Set Lock Message

SECURING DEVICES

4. Use an antivirus program

Windows

- Settings > Update & Security > Windows Security > Virus and Threat Protection
- Good third party options include TrendMicro, Bitdefender, and Norton



Mac

- Still much lower virus threat against Macs, but it is a possibility
- TrendMicro makes a MacOS antivirus
- Also consider creating a non-administrator account for day to day use: System Settings > Users and Groups

SECURING DEVICES

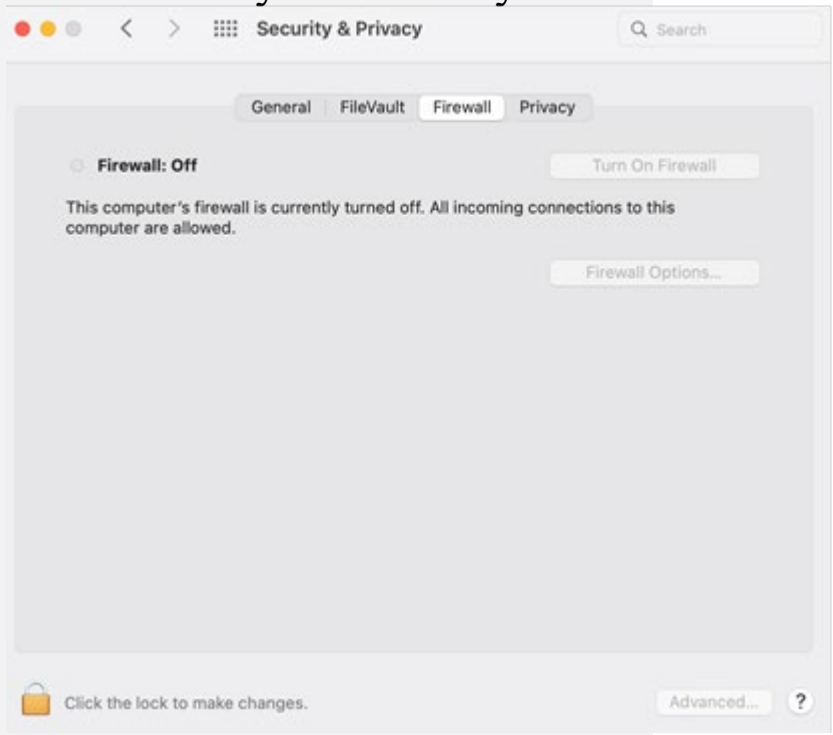
5. Use a firewall

Windows

- Settings > Update & Security > Windows Security > Firewall and Network Protection
- Many antivirus suites will also contain a firewall

Mac

- System Preferences > Security and Privacy > Firewall

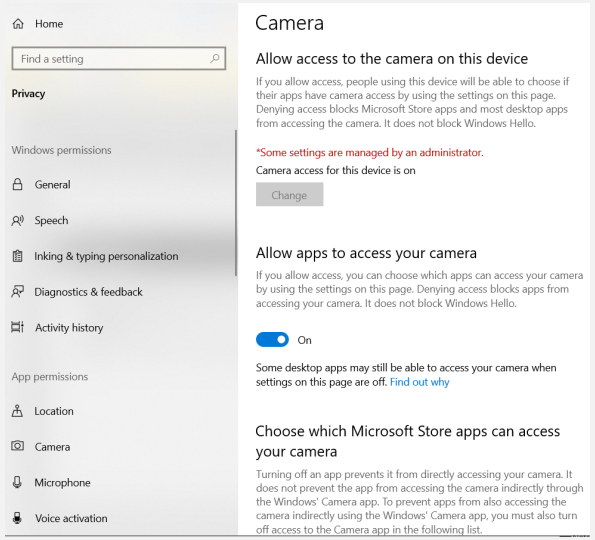


SECURING DEVICES

6. Check your microphone and camera settings

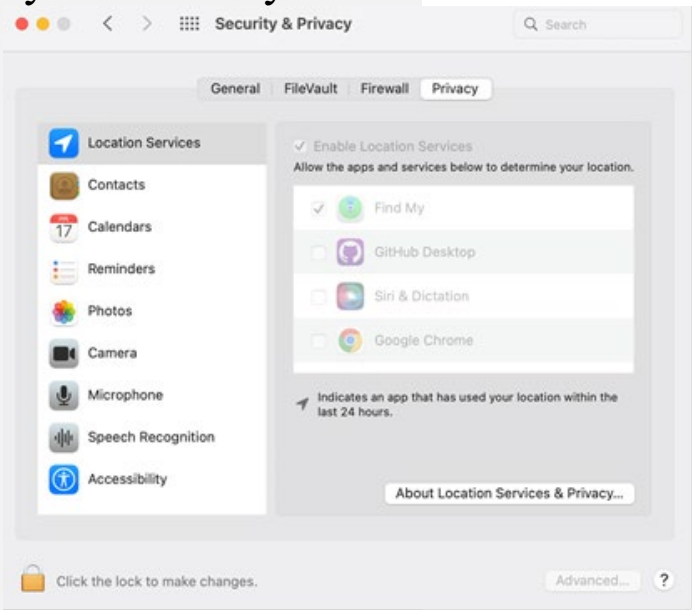
Windows

- Settings > Privacy > Camera
  - Check which apps have access, disable ones you don't need
- Settings > Privacy > Microphone



Mac

- System Preferences > Security and Privacy > Privacy > Camera
- System Preferences > Security and Privacy > Privacy > Microphone



SECURING DEVICES

Smartphones

- Use a password
- Enable screen lock
- Enable device encryption
- Enable a recovery service

SECURING PLATFORMS

- Things like: Gmail, Outlook (MS Exchange), Office365, Dropbox, Box.com, Clio, RingCentral
- Don’t (unduly) fear the cloud
- Use complex, unique passwords
- Enable 2 factor authentication: something you know, something you have
- Review settings for
  - Logon attempts before lockout
  - Account recovery
  - Password complexity and freshness
  - Collaboration/sharing, esp. use of shared links

PASSWORD MANAGERS

- Passwords in iOS
- 1Password
- LastPass
- Guarantee truly complex, unique passwords for all accounts
- Many have “dead hand switch” functionality where a designated contact will be contacted by the vendor to receive access to your credentials if you do not log in within 30, 60, or 90 days
- Easy to manage access for other users
- Easy to change passwords if a service is compromised
- Many also offer an encrypted cloud storage product

VPNS

- Protect against “man-in-the-middle” attacks
- Can by hardware or software
- Review VPN provider company info and privacy terms of use

CYBER LIABILITY COVERAGE

- Generally priced based on number of records/amount of data processed
- Consider types of data you process, e.g. PHI covered by HIPAA
- Breach response, regulatory defense, 3rd party liability
- Available from many insurance companies including TLIE

USER AWARENESS: PHISHING

- Don’t open executable files or unexpected attachments
- Do not provide your login details except on the page to log in to that service
- Check URL by mouseover
- Check for HTTPs
- Displayed email sender info can easily be spoofed- look at the email address domain name, not the sender name
- Be wary of urgency or messages asking not to call
- If in doubt, confirm the request via telephone, using a known number or one obtained from a different source than the message requesting information

USER AWARENESS: GENERAL

- The best tip is on the next slide
- Understand the tools you use
- Subscribe to National Cybersecurity and Communications Integration Center (NCCIC) alerts: *https://www.us-cert.gov/*

JOIN THE COMPUTER AND TECHNOLOGY SECTION TODAY!

The Computer & Tech Section of the State Bar of Texas WANTS YOU!

Is there an easy way to look up Texas statutes, codes and rules from my phone during trial? How can I make my social media presence better? Can I get my clients to sign documents and pay their bill from their smartphone? What is technology competence for attorneys? Membership in the **Computer and Technology Section** can help you answer these questions and more.

We'll help you stay up-to-date on the latest developments in cybersecurity, data privacy, and legal technology, and understand how to use tech to make your practice more efficient and prosperous.

Here's what you need to do— just select Computer & Technology Section box when paying your State Bar Dues or click the link below. It's only $25 and you'll get all of these great member benefits and more:

- **Texas Bar Legal App** accessible on any smartphone (iPhone, Android, web)— full access and keyword search of 62 STATUTES/CODES including Texas and Federal Rules of Procedure and Evidence, Family Code, Estates Code, Penal Code, Civil Practice & Remedies code, and more.
- ***Circuits***, the Section journal which provides practical updates and scholarly analysis on new cases, laws, and technology developments every quarter.
- Attend and participate in multiple legal technology related CLEs in such areas as privacy, cybersecurity, cloud practice management, and attorney technology competence, including our Adaptable Lawyer Track at State Bar of Texas Annual Meeting and annual Access To Justice CLE program.
- Be notified when new micro-CLE videos "**TechBytes**" are released.

JOIN NOW

SBOT.org

FURTHER READING

- NIST NISTIR 7621: https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final
- https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained
- https://thedatamap.org/
- David Sparks the Mac Sparky: https://www.macsparky.com/
- https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/