

LOCK IT DOWN

Build layers of protection so one mistake does not become a disaster.



SECURITY WORKS IN LAYERS

***Remember:** Good cybersecurity plans for human mistakes. The goal is to make one failure insufficient.*

IDENTITY & ACCESS CHECKPOINTS

STRONG, UNIQUE PASSWORDS	Use long, unpredictable passwords or passphrases. Never reuse important passwords across accounts.
PASSWORD MANAGER	Use it to create, remember, autofill, and warn about weak or reused passwords. You remember one strong master password.
PASSKEYS	Use passkeys when available. They replace the password with a credential you unlock on your device or in your password manager.
MFA	Turn on multi-factor authentication. Never approve an unexpected login or approval prompt.
RECOVERY SETTINGS	Keep recovery phones, emails, and backup codes current and protected. Your account is only as secure as the way back in.
APPROPRIATE ACCESS	Give people only the access they need. Remove old employee, vendor, and administrator access promptly.

Protecting Your Practice from Cybersecurity Threats | Part 2

Melissa Hannebrink, Quietech Associates, Inc. | melissa@quietechassociates.com
 John Ellis, Esq., Cybersecurity for the Practice of Law | john@johnellislaw.com



DEVICE CHECKPOINTS

SUPPORTED SYSTEMS	Do not handle sensitive client information on an operating system that can no longer receive security updates.
UPDATES	Install security updates promptly for operating systems, browsers, Office, PDF software, and other commonly used applications.
MALWARE PROTECTION	Keep reputable protection enabled and current on Windows and Mac. Pay attention when it warns you.
STANDARD USERS	Most daily work should not require full administrator rights.
ENCRYPTION	Use BitLocker on Windows or FileVault on Mac, and know where the recovery key is stored.
SCREEN LOCKING	Lock devices when unattended. Use Windows + L on Windows or Control + Command + Q on Mac.
BACKUPS	Back up important data automatically, protect the backup account, keep more than one copy, and test restores.

A stolen laptop should be a hardware loss, not a data breach.

NETWORK & INFRASTRUCTURE CHECKPOINTS

ROUTER AND FIREWALL	Keep firmware updated, change default administrative credentials, and replace unsupported equipment.
WI-FI	Use WPA2 or WPA3, create a separate guest network, and change credentials when access has been widely shared.
PUBLIC WI-FI	Treat networks you do not control as untrusted. Prefer cellular or a hotspot for sensitive work, verify the network name, and do not bypass browser security warnings.
CONNECTED DEVICES	Printers, scanners, storage devices, cameras, and smart devices need updates, strong credentials, and limited access.
REMOTE ACCESS	Use approved tools only, secure unattended access with strong authentication, remove old tools, and never grant access to an unsolicited caller.

Protecting Your Practice from Cybersecurity Threats | Part 2

Melissa Hannebrink, Quietech Associates, Inc. | melissa@quietechassociates.com
John Ellis, Esq., Cybersecurity for the Practice of Law | john@johnellislaw.com



PROCEDURES DECIDE BEFORE YOU NEED THEM

DEFINE ACCESS	Who should have access to which accounts, systems, files, and devices?
DEFINE AUTHORITY	Who can move money, release confidential information, change account settings, or approve unusual requests?
DEFINE VERIFICATION	What requests require independent verification or a second person's approval?
WRITE IT DOWN	Document procedures, make sure everyone knows them, and review them when people, technology, or responsibilities change.

WHAT IF A LAYER FAILS...

SOMEONE CLICKS A BAD LINK	Browser and device protections may block the threat, while limited access and prompt reporting can reduce the damage.
SOMEONE APPROVES THE WRONG THING	Limited privileges may restrict what the attacker can reach.
A LAPTOP IS STOLEN	Encryption protects the data.
SOMEONE REQUESTS A FRAUDULENT WIRE TRANSFER	Your verification procedures stop the payment.

OFFICE REVIEW QUESTIONS

- Which accounts would cause the most harm if compromised?
- Who can approve money movement, account changes, or release of confidential information?
- Which former employees, vendors, devices, or tools may still have access?
- Can the firm restore critical files if ransomware, theft, fire, or hardware failure occurs?
- Does everyone know when to stop and independently verify?

Build layers so one mistake does not become a disaster.

Protecting Your Practice from Cybersecurity Threats | Part 2

Melissa Hannebrink, Quietech Associates, Inc. | melissa@quietechassociates.com
John Ellis, Esq., Cybersecurity for the Practice of Law | john@johnellislaw.com