



~~TRUST, BUT VERIFY~~

SLOW DOWN. VERIFY. THEN TRUST.

The safest habit is not trying to become perfect at spotting fakes.
It is using a process that still protects you when the fake looks real.

WHAT ATTACKERS ARE TARGETING

- **The technology:** software vulnerabilities, malware, ransomware, computers, and networks.
- **The person:** credentials, access, confidential information, money, and decisions.
- **The trust signals we rely on:** familiar names, email addresses, Caller ID, voices, images, logos, and context can be spoofed, compromised, or generated.

THE FIVE TOOLS OF MANIPULATION

FEAR	Creates a threat, then often positions the scammer as the solution.
URGENCY	Gives you a reason to act before you have time to stop and verify.
TRUST	Uses familiarity and believable details to make the request feel authentic.
AUTHORITY	Uses a role, title, expertise, or institution to make compliance feel appropriate.
PRESSURE	Keeps you engaged, isolates you, and makes it harder to question or verify.

Remember: When emotions go up, logic goes down. A legitimate request should be able to survive verification.

SLOW DOWN WHEN THE REQUEST MATTERS

- Money is being sent or moved
- Someone wants access to a computer or account
- Payment or account instructions have changed
- Login credentials or an MFA code are requested
- Confidential information is being requested
- Something feels unusually urgent, secret, or unexpected

BEFORE YOU ACT, ASK YOURSELF

Why do I have to do this right now?	Is someone making it harder for me to stop or verify?	Can I independently verify this specific request?
--	--	--

***A scam does not need to use every manipulation technique.
It only needs enough of them to get the action it wants.***

Protecting Your Practice from Cybersecurity Threats | Part 1

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



E-VERIFICATION PLAYBOOK

Verify independently, using a source you already know is legitimate.

HOW TO VERIFY

1	Leave the channel: Do not verify an email by replying to it, a phone call using a number the caller gives you, or a text by clicking its link.
2	Use a known source: Use contact information already in your records, a number on the back of a bank card, a bookmarked website, or another independently obtained source.
3	Contact them directly: Reach the person or organization through that trusted channel.
4	Verify the specific request: Confirm the exact action being requested, not merely the identity or existence of the person.
5	Act only after confirmation: If you cannot independently confirm it, do not proceed with the sensitive action.

EXAMPLES

“Sarah” emails new wiring instructions	Call Sarah using a number you already have and ask, “Did you send me new wiring instructions?”
“Microsoft” emails about an account problem	Do not click the provided link. Go independently to Microsoft or contact your known IT provider.
“Michael” calls with an urgent request	Contact Michael through a method you already know belongs to him, especially if the voice could be cloned.

OLD HABIT	NEW HABIT
“Does this look real?”	“Can I independently verify it?”

TAKEAWAYS

- Cybersecurity is not only about technology. Attackers may target the person instead of the computer.
- Familiar does not mean authentic. Email addresses, Caller ID, voices, images, and context can all be faked or compromised.
- Recognize the manipulation: fear, urgency, trust, authority, and pressure.
- Slow down when money, credentials, access, confidential information, or changed instructions are involved.
- Verify independently. Verify the request, not just the message or the apparent sender.

**You do not have to recognize every scam.
You need a process that still protects you when you do not.**

Protecting Your Practice from Cybersecurity Threats | Part 1

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