SOCIAL ENGINEERING

Protecting your practice, your clients and their money

SOLE & SMALL FIRMS

Risks • Controls • Red flags • Response



A transfer request arrives at 3:45 p.m.

Closing is today. The email thread is genuine. The banking instructions are not.



Would you authorize it?

- ? Looks like the client
- ? Appears inside the existing thread
- ? Explains the urgency
- ? Provides “revised” account details

The question is not “Does it look real?”
The question is “How was it independently verified?”

Social engineering targets decisions, not devices

Deception is used to make a reasonable person take the wrong action.

Reveal

Credentials
Security codes
Confidential client information

Act

Open a link
Change contact details
Bypass a normal procedure

Transfer

Trust money
Property or settlement proceeds
Payments to a false account

The fraudster wins when urgency or familiarity replaces verification.

Why small practices are attractive targets

High-value information and money, often moving through lean processes.

TRUST FUNDS

Large, time-sensitive payments

CLIENT DATA

Enough context to impersonate convincingly

LEAN TEAMS

Limited segregation of duties

DEADLINES

Closing pressure rewards speed

INFORMALITY

Familiar clients can reduce skepticism

ONE DECISION

One person may initiate and release

How the fraud unfolds

A patient sequence designed to make the final instruction feel normal.



Research

Matter, parties, timing

Access

Compromise or imitate

Observe

Learn the conversation

Intervene

Send revised instructions

Pressure

Urgency, secrecy, closing

Transfer

Money goes to fraudster

The decisive message may be the last step of a much longer compromise.

Where it appears in legal practice

The pattern changes, but the control principle stays the same.

Changed banking instructions

Client or beneficiary

Altered payout statement

Lender or opposing party

Fake lawyer direction

Assistant or bookkeeper

Credential lure

Document portal or security notice

Bad-cheque retainer

New “client” and urgent payout

Invoice substitution

Vendor or expert

Red flags in the instruction

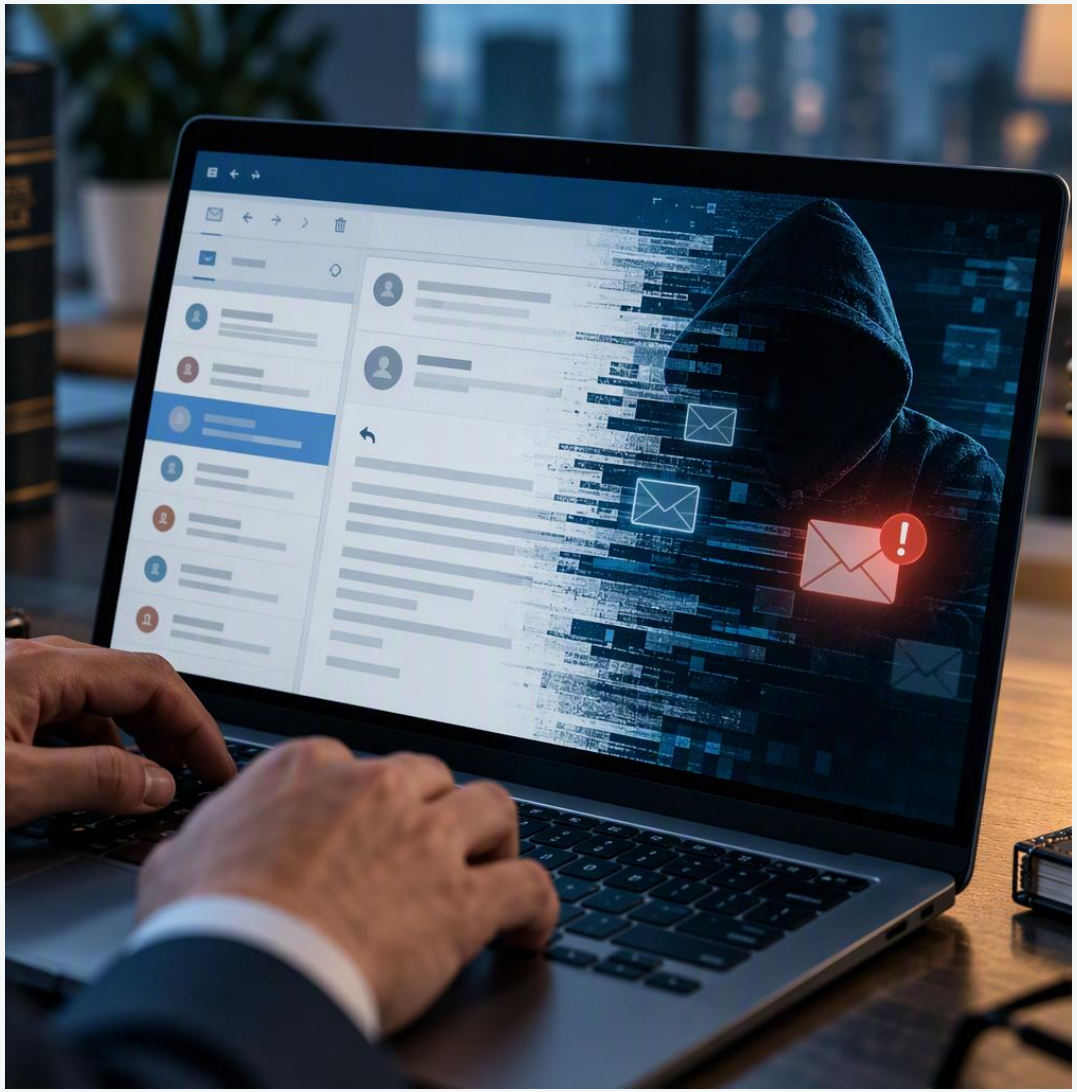
Any one may be explainable. Several together should stop the transaction.

- **New or revised payment details**
- **Last-minute account or jurisdiction change**
- Payment to an unexpected third party
- Split payments across multiple accounts
- Reason normal verification “cannot” occur
- Urgency, secrecy or pressure to bypass process
- Instructions inconsistent with the retainer
- Resistance to independent confirmation

Red flags in the communication

Look beneath the display name and the familiar thread.

- **A swapped character in the domain**
- **Different address behind the display name**
- Change in tone, terminology or sign-off
- A participant disappears from the thread
- New phone number supplied with new banking details
- Unexpected attachment, QR code or login page



The control stack

Simple controls, consistently applied, create several chances to stop the fraud.

1	**Set expectations**	Retainer explains how funds instructions will be exchanged
2	**Freeze email-only changes**	No banking change is accepted by email alone
3	**Verify independently**	Call a previously established number
4	**Separate preparation and release**	Second review where practical
5	**Secure access**	MFA, unique passwords, updates, restricted admin rights
6	**Monitor**	Alerts, prompt reconciliation, review of unusual activity

Independent verification is the critical control

Do not use the contact information contained in the instruction being verified.



1. Initiate

You place the call. Do not rely on an incoming call.

2. Use a trusted source

Call a number already on file or obtained from a reliable directory.

3. Record the result

Document who confirmed, when, how and exactly what was confirmed.

CHANGE = AUTOMATIC STOP

STOP • VERIFY • DOCUMENT

A rule that works under closing pressure.

1

STOP

Pause every new, changed, urgent or unusual instruction.

2

VERIFY

Use a previously established, independent channel.

3

DOCUMENT

Record the request, call-back, approval and release.

Before releasing funds

A one-minute checklist can prevent a six-figure loss.

- [ ] Authorized by the retainer and client instructions
- [ ] Appropriate person had authority to confirm
- [ ] Recipient and purpose are expected
- [ ] Amount and destination reviewed
- [ ] Banking details match verified information
- [ ] Second approval obtained where required
- [ ] Every change independently confirmed
- [ ] Verification and approval documented
- [ ] Established contact information used
- [ ] Confirmation reviewed promptly

If something seems wrong

Speed matters. Begin containment before every fact is known.

BEFORE FUNDS LEAVE

- ✓ Stop the transaction
- ✓ Move outside the suspected email chain
- ✓ Contact the client or party independently
- ✓ Preserve messages, headers and documents
- ✓ Secure potentially compromised accounts

AFTER FUNDS LEAVE

- ! Call the bank immediately
- ! Request stop, recall or freeze
- ! Notify insurers and incident-response support
- ! Assess regulatory and privacy reporting
- ! Communicate carefully with affected parties

Cyber insurance: social engineering cover

A big headline limit does not mean a big payout. Typical market ranges; confirm actual terms with your broker.

WHAT TO LOOK FOR

- ✓ Social engineering cover expressly named
- ✓ Sublimit sized to your largest transfer
- ✓ Verification conditions you can really meet
- ✓ Client and trust funds confirmed as covered
- ✓ No gaps or overlap with your crime policy

SUBLIMIT WATCH-OUTS

- ! Often $25K–$250K, far below policy limit
- ! A sublimit can cap the entire loss
- ! Skipped callback verification can void claim
- ! May apply excess of any crime policy
- ! Strong controls can justify a higher sublimit

Read the sublimit, not just the policy limit.

Five commitments for the next 30 days

Small changes that materially improve the safety of the practice.

1. **Add funds-transfer language to retainers**
2. **Ban email-only changes to payment instructions**
3. **Use a standard verification checklist**
4. **Enable MFA and review account security**
5. **Review insurance conditions and incident contacts**

Trust the person. Verify the transaction.

THANK YOU
QUESTIONS?

Trust the person. Verify the transaction.

DISCUSSION

Stop • Verify • Document

