PROTECTING YOUR IDENTITY AND FINANCIAL SECURITY

Practical guidance for safeguarding your accounts, personal information, and financial life.

In today's environment, financial fraud is not just more common – it is more convincing. Messages are designed to appear familiar, credible, and urgent. Emails can mirror trusted institutions, phone calls may seem to come from know contacts, and requests often feel routine. Protecting your financial life comes down to three consistent disciplines: **Protect. Verify. Monitor.** When applied thoughtfully, these habits can significantly reduce exposure to identify theft, account compromise, and fraudulent transactions.

PROTECT Your Access and Personal Information

Your login credentials and personal data are the most common entry points for fraud.

- Use unique and complex passwords for every account
- Enable multi-factor authentication (MFA) – especially for email and financial platforms
- Do not store passwords in shared devices or unsecured notes
- Avoid logging into accounts over public Wi-Fi (airports, hotels, etc.)
- Keep phones and computers up to date
- Install only trusted apps

Be selective and thoughtful with personal information:

- Do not share Social Security numbers, account numbers, or login credentials unless truly necessary
- Limit personal details posted publicly (birthdates, addresses, travel plans)
- Shred physical documents that contain sensitive information

Most Fraud begins with access. Limiting exposure is the first line of defense.

VERIFY Before Taking Action

Fraud normally involves deception – requests that appear legitimate but are not.

Be cautious of:

- Emails or Texts that create urgency: "Act Now," "Account Compromised," "Payment Required Today"
- Messages that look like they're from your advisor, custodian, or bank – but contain slight differences in spelling or domain (e.g. .co vs .com)
- Unexpected attachments (PDFs, DocuSign links, invoices)
- Requests to move money, change wiring instructions, or update account details
- Requests to shift communication to text, WhatsApp, or another platform

Always verify independently:

- Confirm any money movement by request by calling a known, trusted number – not one provided in the message
- If something appears legitimate but unexpected, contact the known sender directly before responding

Taking a moment to verify is often the difference between avoiding an issue and dealing with one.

— continued on next page

MONITOR Your Accounts and Activity

Consistent awareness remains one of the most effective safeguards.

- Review account activity regularly – even small or unfamiliar transactions
- Enable alerts for logins, withdrawals, and profile changes

Pay attention to:

- Password reset emails you didn't request
- Notifications of new devices accessing your account
- Missing statements or unexpected changes in communication

If something doesn't look right

- Act promptly – delays increase potential impact
- Change passwords and secure accounts
- Contact your banker, advisor, or financial institution directly

Common situations to watch for:

- **Wire fraud:** You receive updated wiring instructions shortly before a transaction
- **Account impersonation:** Someone poses as your advisor or institution requesting information
- **Email compromise:** A familiar contact sends an unusual or out-of-character request
- **Phishing links:** A message directs you to log in through a link instead of your usual site
- **Credential Theft:** A data breach leads to login attempts across multiple accounts

Secure how you communicate:

- Use secure client portals for documents whenever possible
- Avoid sending account details or sensitive information via standard email or text
- Be cautious with file-sharing links or unexpected document requests

IF SOMETHING FEELS OFF...

- Pause – do not act on the request
- Contact your banker, advisor, or institution using verified contact information
- Secure your accounts IMMEDIATELY if needed

We view security as an ongoing discipline – not a reaction.
The most effective protection comes from simple consistent habits – protecting access, verifying requests, and staying attentive to activity. Applied over time, these practices create a meaningful layer of protection against even the most sophisticated attempts.

PROTECT. VERIFY. MONITOR.

CALLAHAN FINANCIAL
MANAGEMENT GROUP, LLC

7495 Paragon Rd, Suite A | Dayton, OH 45459
(937) 432-9100 | **www.callahanfinancialmg.com**