Bahl&Gaynor
Dividends Pay Dividends®

Protecting Your Personal Information

Cybersecurity Tips for Clients

Cybercrime and financial scams continue to increase across the financial industry. Many modern scams rely on psychology, urgency, and impersonation rather than sophisticated hacking. High-net-worth individuals are often targeted because of their assets, investments, and authority.

At Bahl & Gaynor, protecting our clients' personal and financial information is a priority. The following guidelines provide practical steps you can take to help safeguard your accounts and personal data.

PROTECTING YOUR INFORMATION

Use Strong Passwords
Create unique passwords for each financial account. Consider using a password manager to store them securely.

Enable Multi-Factor Authentication
Whenever available, enable multi-factor authentication for financial accounts, email, and other sensitive services.

Monitor Your Accounts
Regularly review bank, credit card, and investment account activity and report suspicious activity promptly.

Keep Devices Updated
Install updates for computers, tablets, and smartphones to maintain the latest security protections.

Consider a Credit Freeze
A credit freeze restricts access to your credit report, making it more difficult for identity thieves to open accounts in your name.

You can place or lift a freeze at any time with the three major credit bureaus:
- Equifax – www.equifax.com | 800 • 349 • 9960
- Experian – www.experian.com | 888 • 397 • 3742
- TransUnion – www.transunion.com | 888 • 909 • 8872

This is one of the most effective tools to prevent new account fraud.

BE CAUTIOUS WHEN

Clicking Links in Emails OR Text Messages
Phishing emails remain the most common entry point for fraud. Criminals often impersonate banks, advisors, investment platforms, or charities.

If you receive an alert about account activity:
- Do not click links in the message
- Instead, log on to your personal account through the direct website or mobile app

Evaluate Personal Cyber Insurance
Some homeowners or specialty insurance policies offer coverage for cyber-related losses, including fraud, identity theft, and data breaches.

Coverage may include:
- Reimbursement for stolen funds
- Identity restoration services
- Legal or forensic support

Consider discussing options with your insurance provider.

Understand Banking & Check Reporting Systems
Banks use reporting systems such as ChexSystems and Early Warning Services (EWS) to track account activity and detect potential fraud.

Why this matters:
- Fraudulent accounts opened in your name may be reported in these systems
- This could impact your ability to open new bank accounts

What you can do:
- Periodically request a copy of your report
- Review for unfamiliar or inaccurate activity
- Report discrepancies promptly

Limit Check Fraud Risk
If you use checks, ask your bank about fraud protection tools such as:
- Positive Pay – verifies checks before they are processed
- Check restrictions or blocking services – limits check activity on your account
- Transaction alerts – notifies you of account activity

If you rarely write checks, consider restricting check activity on your account.

This information is provided for educational purposes to help clients better understand common cybersecurity risks and protective measures.

continued >

Receiving Urgent or Emotional Requests
Fraudsters often create urgency or emotional pressure to push victims into acting quickly.

Examples include:
- Emergency requests from a "family member"
- Calls from someone claiming to be a lawyer or advisor
- Urgent account alerts demanding immediate action
- Texts from government agencies

Always pause and verify the request through a trusted contact number.

Changes to Wire Instructions
Criminals frequently monitor email accounts and send last-minute messages requesting updated wire instructions for large transactions such as real estate closings or investments.

Always confirm instructions sent by wire with a phone call by using a known number before sending funds.

Check Washing and Mail Theft
Check washing occurs when criminals steal checks and alter the payee or amount.

To reduce risk:
- Avoid leaving outgoing mail in unsecured mailboxes
- Use secure USPS collection boxes or post offices
- Monitor accounts for unauthorized check activity
- Consider electronic payments when possible

Tax Return Fraud
Fraudsters may attempt to file a tax return in your name to claim a refund.

Warning signs include:
- Receiving IRS notices about returns you did not file
- Being told a return has already been submitted

To help protect yourself:
- Consider obtaining an IRS Identity Protection PIN (IP PIN)
- Safeguard Social Security numbers and tax documents

Investment Opportunities That Seem Too Good to Be True
Fraudsters increasingly create professional-looking websites, social media promotions, or "exclusive" investment opportunities designed to appear legitimate.

Be cautious if an opportunity includes:
- Guaranteed returns
- Pressure to act quickly
- Requests to transfer funds to unfamiliar platforms
- Requests to convert assets to cryptocurrency

Always consult your advisor before moving funds to a new investment.

IF YOU SUSPECT IDENTITY THEFT

If you believe your personal information may have been compromised:

1. Contact your financial institutions immediately.
2. Place a fraud alert or credit freeze with the major credit reporting agencies.
3. Report the incident to the Federal Trade Commission at www.IdentityTheft.gov.
4. Monitor your accounts closely for unauthorized activity.

Taking action quickly can help limit potential damage.

HELPFUL RESOURCES

1. Federal Trade Commission – Identity Theft
   www.identitytheft.gov
2. IRS Identity Theft Information
   www.irs.gov
3. U.S. Government Identity Theft Resources
   www.usa.gov/identity-theft
4. ChexSystems Consumer Report
   www.chexsystems.com
5. Early Warning Services
   www.earlywarning.com

This information is provided for educational purposes to help clients better understand common cybersecurity risks and protective measures.