

## Foiling the Financial Fraudsters:

### *How to Protect Yourself from Scams*

Financial scammers are constantly looking for ways to steal from those of us with significant assets. Unfortunately, they are often more successful than we think.

Even if you are financially savvy or cautious about who you trust, it doesn't mean scammers won't target you or that you'll be able to completely avoid their traps.

With that in mind, here are some common ways scammers might target you, and how you can avoid falling victim to their schemes.

#### *You're a Target*

Scammers often focus on wealthy individuals. In fact, the affluent are 43% more likely to be victims of identity theft, according to research by Experian and the Department of Justice.

**The good news:** You can take steps to protect yourself from financial scams. Start by learning about the various ways scammers try to steal from you and the damage these scams can cause.

#### *Common Scams to Watch For*

**Phishing and Ransomware:** Phishing is when scammers pose as legitimate companies through fake emails or texts, tricking you into sharing personal information. Ransomware is malicious software that locks your files until you pay a ransom to regain access. While ransomware often targets big companies, 82% of attacks now target small businesses that may have weaker security.

**Wire Transfer Fraud:** This happens when scammers trick you into wiring money, often by posing as someone you trust. For example, real estate investor Barbara Corcoran lost nearly \$400,000 when scammers pretending to be her assistant convinced her bookkeeper to wire money for a fake investment.

**Account Takeovers:** In this type of identity theft, scammers gain unauthorized access to your accounts, often by setting up fake public Wi-Fi networks to steal usernames and passwords.

#### *How to Avoid Getting Scammed*

Now that you know some common scams, here are steps you can take to protect yourself:

##### **1. Strengthen Your Basics**

Secure your home network, use strong passwords, set up multi-factor authentication, and install security software. These basic steps form the foundation of your protection.

##### **2. Slow Down and Be Cautious**

Scammers often create a sense of urgency to push you into quick decisions. Take your time and investigate any requests thoroughly. Make sure your financial team—advisors, bookkeepers, etc.—double-checks any urgent financial requests with you.

### **3. Verify Requests Directly**

If you get an unexpected email or text from your bank or another institution, don't click on any links. Contact them directly to confirm whether the request is legitimate.



### **4. Watch Out for Impersonators**

Scammers may create fake social media profiles to gather personal information. Report any fake accounts, verify friend requests, and avoid responding to messages from strangers.

### **5. Separate Work and Personal Life**

If you're a business owner, use separate emails for personal and business communication. This can help prevent a breach in one area from affecting the other.

### **6. Monitor Your Finances**

Regularly review your financial statements and credit reports for any unusual activity. This won't stop fraud, but it can help you catch it early.

### **7. Don't Be Afraid to Ask for Help**

If you think you've been scammed or are unsure about a situation, seek help from authorities or trusted advisors. Don't let embarrassment stop you from protecting yourself.

Remember, many of the most effective ways to avoid scams depend on your actions, not just technology. Combining smart behavior with tech tools will greatly reduce your risk of becoming a victim.