Digital Pump and Dump: How Scammers Target Retirees on Social Media

Uncover the tactics behind digital "pump and dump" schemes, including identity theft and fake investment opportunities on platforms like WhatsApp, and learn protection strategies.

RETIREMENT DAILY GUEST CONTRIBUTOR • APR 7, 2025 7:00 AM EDT

By John O'Connell

Retirement Daily | On TheStreet

Investors and retirees face sophisticated threats that combine social engineering with technology on social media. One of the most persistent schemes targeting unsuspecting investors is the "pump and dump" scam, which has found new life on messaging platforms like WhatsApp. This article examines how these schemes work, and the techniques cybercriminals use to execute them.

Understanding Pump and Dump Schemes

A pump and dump scheme is a form of securities fraud where cybercriminals artificially inflate the price of an owned stock through false and misleading positive statements, then sell their shares at the inflated price before the inevitable market correction occurs. These schemes typically target microcap stocks, penny stocks, and cryptocurrencies that have low liquidity and limited information available to investors.

The mechanics of a pump and dump operation follow a predictable pattern:

1. **Accumulation**: Cybercriminals quietly acquire a substantial position in a low-priced, thinly-traded stock.
2. **Promotion**: They create buzz around the stock using misleading claims about potential breakthroughs, contracts, or acquisitions that don't exist or are grossly exaggerated.
3. **Price inflation**: As unsuspecting investors purchase shares based on false information, increased demand drives the price up artificially.
4. **Dumping**: Once the price has risen sufficiently, the cybercriminals sell their shares at the inflated price.
5. **Collapse**: Without the artificial support, the stock price plummets, leaving legitimate investors with significant losses.

The traditional pump and dump relied on cold calling or newsletter promotions. Today's digital version uses social media platforms, messaging apps, and impersonation tactics to reach potential victims while creating a false sense of legitimacy.

Digital Identity Theft: Harvesting Financial Advisors' Information

Cybercriminals begin by identifying targets who possess credibility in the financial sector. Licensed financial advisors make ideal candidates because they have professional credentials and established trust with investors.

The information gathering process is surprisingly straightforward:

1. **Financial firm websites**: Most financial advisory firms prominently display their advisors' profiles, including professional headshots, biographical information, and credentials. These pages are designed to build client trust but inadvertently provide cybercriminals with valuable source material.
2. **Regulatory databases**: Financial advisors' credentials can be verified through public databases like FINRA's BrokerCheck or the SEC's Investment Adviser Public Disclosure website, which contain detailed professional backgrounds.
3. **Social media research**: Professional platforms like LinkedIn provide additional details about an advisor's career history, education, and professional accomplishments.

4. **Data aggregation**: Cybercriminals may cross-reference information from multiple sources to create comprehensive profiles.

5. **Reverse image search protection failure**: Many advisors' professional headshots lack digital watermarks or other protections that would prevent their unauthorized use.

Cybercriminals select advisors who have established reputations, especially those with substantial client bases or those who specialize in the types of investments the fraudsters plan to promote. By impersonating known, trusted professionals, scammers greatly increase their chance of success.

Creating Convincing WhatsApp Impersonations

With the target's information secured, cybercriminals create convincing WhatsApp profiles that appear legitimate even to cautious observers:

1. **Profile creation**: Setting up a WhatsApp account requires only a phone number, which cybercriminals obtain using prepaid phones or VoIP services that provide temporary numbers, making them difficult to trace.

2. **Profile picture**: The stolen professional headshot is added as the WhatsApp profile picture, creating immediate visual legitimacy.

3. **Status and bio**: Cybercriminals add professional descriptions matching the advisor's actual credentials and specialties, often copied directly from firm websites or LinkedIn profiles.

4. **Building credibility**: Before pitching investments, scammers establish rapport by sharing general market analysis or publicly available information about mainstream stocks, creating an impression of expertise.

5. **Contact lists**: Victims may be identified through data breaches, public forums, or social engineering, allowing cybercriminals to target people who might be interested in investment opportunities.

6. **Group dynamics**: Creating investment discussion groups provides social proof, as potential victims see others (often fake accounts) appearing to engage with and trust the impersonated advisor.

Once the groundwork is laid, the cybercriminal sends messages about "exclusive opportunities" in penny stocks, often framing them as limited time offers to create urgency. They may claim to have insider information or special insight into upcoming developments that will cause the stock to skyrocket.

Protecting Yourself from Digital Pump and Dump Schemes

Investors and retirees can protect themselves by verifying advisors through official channels before engaging in investment discussions. Legitimate financial advisors typically communicate through regulated, official channels rather than WhatsApp or similar platforms.

Remember that genuinely lucrative investment opportunities rarely come through unsolicited messages, and claims of guaranteed returns or pressure to act quickly are classic red flags of fraud.

Financial advisors should monitor their online presence and consider using digital watermarks on professional photos. Firms should implement verification procedures that allow clients to confirm communications are authentic.

By understanding how these schemes operate in the digital realm, investors can better protect themselves from becoming victims of these increasingly sophisticated financial frauds.

John O'Connell is founder and CEO of The Oasis Group, a leading consultancy for the wealth management industry that specializes in helping wealth management and technology firms solve their most complex challenges. The Oasis Group offers award-winning consulting services, industry-leading research, and compelling on-demand training for wealth management firms and the service providers who serve the wealth management industry. The firm's newest online training courses serve as a leading source of education for financial professionals at all levels in their careers.