



Protect Yourself from Targeted Scams

Fraudsters are increasingly impersonating trusted companies, including Schwab, to exploit trust and access personal information.

Here's how to recognize and safeguard against these scams:

Common Scams and How They Work

1. **Urgent Communications:** Scammers use phone, email, text, or social media to create a sense of urgency, pressuring you to click links, call fake numbers, or grant remote access. These tactics lead to stolen credentials or malware installation.
2. **Impersonation of Trusted Experts:** Fraudsters pose as legitimate financial professionals, often using real employee names and titles and offering "exclusive" investment opportunities via unsolicited messages.
3. **Fake Websites:** Scammers create fake websites resembling trusted institutions. These sites capture login credentials or display fraudulent alerts prompting victims to contact fake support lines.

How to Protect Yourself

- **Use Official Channels:** Access accounts directly through verified websites or mobile apps, avoiding links in unsolicited communications.
- **Verify Phone Numbers:** Independently confirm phone numbers through trusted sources like official websites or account statements.
- **Enable Two-Factor Authentication:** Add an extra layer of security to your accounts whenever possible.
- **Bookmark Trusted Websites:** Save official websites to avoid relying on search results, which may include fake sites.
- **Stay Skeptical of Urgent Requests:** Pause and verify before acting on unexpected or rushed demands.
- **Guard Your Information:** Never share sensitive details like passwords or one-time security codes with anyone contacting you unexpectedly.