



## EMERGING FRAUD TREND: HOSTILE EMAIL ACCOUNT TAKEOVER

Do you know who is on the other end of that email address? It might not be as apparent as you think.

One area of fraud which has seen a significant increase in activity is email hacking. In this type of fraud, an unauthorized person uses malware—such as a keystroke-logging or "keylogging" program—to take control of a victim's email account, often by secretly stealing their email login credentials. The fraudster can then send messages from the account or even monitor incoming messages to identify any financial institution(s) with which the victim does business.

Fraudsters find email-related schemes appealing and effective because email is a common form of communication and provides a layer of anonymity, making it easier to leverage the trust of the relationship.

Listed below are some suspicious signs that may indicate that you are receiving a message from a hacked account:

- Originating email address is not the true email address or originating email address changes during the course of emails  
**Example:** A lowercase "l" and a capital "I" can sometimes be indistinguishable.
- Originator makes an urgent request to send a wire to a third party.  
**Example:** Fraudster requests a wire be sent in U.S. dollars to bank in Hong Kong because of a death in the family.
- Originator states that he or she is unavailable by phone.  
**Example:** The email states that he or she is out of the country, about to board an airplane, at the hospital, attending a funeral, and so on.
- Time zone stamp on the email does not match the victims geographic location.  
**Example:** Victim lives in on the East Coast, but the email time stamp does not correspond.

# Client Alert...Client Alert...Client Alert

Listed below are some best practices that will protect you against email fraud:

- Pay attention to spelling and grammatical errors, as well as the tone of email communications.
- Pay attention to suspicious signs whenever you are asked to rush a request. Fraudsters will sometimes use a frightening or disturbing event to establish an emotional attachment and then ask that a request be expedited.
- Do not open attachments from senders you do not know.
- Never provide your account numbers, passwords, or social security number in response to an email request.
- Make sure that your computer's operating system and all of its software is set to automatically update.
- Activate your computer's firewall.
- Install anti-virus software and keep it up to date.
- Install anti-spyware software and keep it up to date.
- Do not open attachments from unreliable sources.
- Use extra caution when using a public computer or logging onto public networks away from your home.

If you happen to get an email that you believe is fraudulent, you should not open the message or any of its attachments nor should you click any links within the body of the email. Delete the email from your inbox and again from your deleted items folder.

(Source: Charles Schwab & Co., Inc.)

**Powers Capital Investments, Inc. is a registered investment adviser.**

**This publication is only intended for clients and interested investors residing in jurisdictions in which the Adviser is qualified to provide investment advisory services. The Adviser does not attempt to furnish personalized investment advice or services through this publication. Any subsequent, direct communication with a prospective client will be conducted by the Adviser's investment advisory representatives. Some of the information given in this publication has been produced by unaffiliated third parties and, while it is deemed reliable, the Adviser does not guarantee its timeliness, sequence, accuracy, adequacy, or completeness and makes no warranties with respect to results to be obtained from its use.**

**To unsubscribe to this Client Alert, please send an email to [unsubscribe@powerscapital.com](mailto:unsubscribe@powerscapital.com)**

# Client Alert...Client Alert...Client Alert