

## **Darien Police Offer Businesses Tips on Avoiding Wire Fraud**

**Author :** David Gurliacci

**Categories :** [Business](#), [Public Safety](#)

**Tagged as :** [Business Email Compromise Scam](#), [Business Email Compromise Scam 2015](#), [Business Email Scam](#), [Business Email Scam 2015](#), [Crime Prevention Tips](#), [Crime Prevention Tips 2015](#), [Darien Police Department](#), [Darien Police Department 2015](#)

**Date :** December 8, 2015



Darien police have just offered tips on how to avoid having your business become a victim of wire fraud.

Recently, two Darien businesses — a travel agency and a real estate business — were scammed by hackers who got into a top executive's email account and issued directives to have money wired.

The travel agency [lost \\$10,000](#). The real estate business [lost \\$48,600](#).

*Here's the complete tip sheet, [as posted on Facebook](#) by Darien police:*

### **Town of Darien Business Alert System**

Issued by: Det. Sgt. Jeremiah P. Marron Jr.

The Darien Police Department has received a recent increase in “business e-mail compromise” complaints. According to the FBI, most companies that have fallen victim to these types of scams receive an email asking an accountant or someone else with access to corporate funds to send urgent wire transfers to accounts under

the control of the scammers.

The fraudulent e-mail appears to have originated from an executive within the company and includes an attachment with instructions for the wire transfer.

According to the 2015 Payments Fraud and Control Survey from the Association for Financial Professionals, about 3 in 5 businesses are targets of payments fraud and typically sustain an average of \$130,000.00 in losses.

The Darien Police Department is offering these tips to reduce the risk of falling victim to this type of scam:

- Be suspicious of wire transfer requests that ask for quick action or secrecy.
- Limit the number of employees within your business who have the authority to approve and/or conduct wire transfers.
- Verify a change in payment instructions to a vendor or supplier by calling to verbally confirm the request.
- Use authentication protocols to verify wire transfer requests that are seemingly coming from executives. This may include calling the executive to obtain verbal verification, establishing a PIN to verify the executive's identity, or sending the executive via text message a one-time code and a phone number to call in order to confirm the wire transfer request
- Lastly, require a 2-step verification process or dual-approval for any wire transfer request involving a dollar amount over a specific threshold

If your business falls victim to this type email scam, report it immediately to the Darien Police Department,

***Darienite***

***News for Darien***

***<https://darienite.com>***

---

your financial institution, the institution where the transaction was sent, and the FBI's Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov) .

By following these protocols the likelihood to recover losses is increased. Thank you for your cooperation.