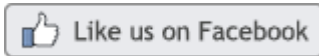


## FEA MEMBER ALERT



### QIs Targeted by Cyber Criminals

#### FEA STAFF

##### Executive Director

Lynn Harkin, CAE  
*Certified Association Executive*  
FEA  
1255 SW Prairie Trail Pkwy.  
Ankeny, IA 50023-7068  
(515) 244-6515 Office  
(515) 334-1067 Direct  
(515) 334-1167 Fax  
[director@1031.org](mailto:director@1031.org)  
[www.1031.org](http://www.1031.org)

#### EARN YOUR CES® DESIGNATION



[Learn More](#)

Dear FEA Members:

As reported at the FEA's Annual Conference in Nashville last month, the 1031 industry is a direct target of wire fraud and cyber hacking schemes designed to access exchange funds.

Multiple FEA members have been the target of sophisticated and individualized efforts to inject fraudulent wire instructions and disbursement requests into the flow of specific transaction communications.

Additionally, a recent email soliciting accommodators under the pseudonym **Antwain Howell** was sent to multiple members of the FEA.

Upon responding to the inquiry, the sender attaches a file containing a computer virus under the appearance of being a file containing exchange documents.

These computer viruses are created to track keystrokes, passwords and processes, exert control over computer systems and in many cases hijack a computer system.

Other instances of fraud have included persons posing as potential buyers of QI companies and a fraudulent email offering bank depository services.

This alarming increase in cases targeting accommodators appears to be the result of recent publicity concerning the industry.

Continuing efforts to target our industry are a certainty for the ongoing future.

It is critical that FEA member companies make all possible efforts to safeguard their computer networks, implement safety processes and be hyper vigilant of fraudulent activities.

To learn how to protect yourself from wire fraud schemes, refer to the August 8, 2014, FEA alert email to members.

Other tips to avoid becoming the victim of cybercrime may be viewed at the following links:

FBI: [http://www.fbi.gov/scams-safety/fraud/internet\\_fraud](http://www.fbi.gov/scams-safety/fraud/internet_fraud)

Internet Crime Complaint  
Center: <http://www.ic3.gov/preventiontips.aspx>

Microsoft: <http://www.microsoft.com/security/default.aspx>

Symantec: <http://us.norton.com/prevention-tips/article>