

Details: EXTORTION EMAIL

The FBI has been made aware of a spam email attempting to extort money from professionals, including bankers, dentists, and doctors, using the professionals personal email accounts. In this "spear phishing" scam, scammers target a specific group of people. The email purports to be from a "hitman" and provides accurate information about the victim including complete name. The email threatens to complete his contract unless the victim sends \$80,000. The email alleges that once the money is received, the victim would be safe. It further advised the victim would never hear from the sender again.

Example of email text.

*"Good day,
I want you to read this message very carefully, and keep the secret with you till further notice, You have no need of knowing who i am, where am from, till i make out a space for us to see, i have being paid \$50,000.00 in advance to terminate you with some reasons listed to me by my employers, its one i believe you call a friend, i have followed you closely for one week and three days now and have seen that you are innocent of the accusation, Do not contact the police or F.B.I. or try to send a copy of this to them, because if you do i will know, and might be pushed to do what i have being paid to do, beside, this is the first time I turned out to be a betrayer in my job.
Now, listen, i will arrange for us to see face to face but before that i need the amount of \$80,000.00 and you will have nothing to be afraid of. I will be coming to see you in your office or home determine where you wish we meet, do not set any camera to cover us or set up any tape to record our conversation, my employer is in my control now, You will need to pay \$20,000.00 to the account i will provide for you, before we will set our first meeting, after you have make the first advance payment to the account, i will give you the tape that contains his request for me to terminate you, which will be enough evidence for you to take him to court (if you wish to), then the balance will be paid later....."*

The FBI's Internet Crime Complaint Center received reports about this particular scam in early December 2006 and again in October 2007.

Loss Prevention Recommendations:

- **These emails are an attempt to extort money. Do not follow the instructions.**
- Do **not** correspond with the sender.
- Report receipt of email to local law enforcement and FBI.
- Be cautious - protect personal identity when responding to requests or special offers delivered through unsolicited email.
- Guard your personal information as well as your account information carefully.
- Keep a list of all your credit cards and account information along with the card issuer's contact information.
- If your monthly statement looks suspicious or you lose your card(s), contact the issuer immediately.
- If you have received this, or a similar hoax, please file a complaint at www.ic3.gov.

If you are aware of a risk in your area, whether it has struck your credit union or not, please complete the [Report a RISK Alert](#) form.

The information contained in this RISK Alert is intended for the sole use of our Credit Union Bond policyholders to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

CUNA Mutual Group does not provide any warranties or guarantees with respect to the performance of services by any vendor, and is not liable for any products or services purchased from any vendor by any credit union. Each credit union is ultimately responsible for determining the products and services that it may require, selecting the vendor that best meets the credit union's needs (whether or not a preferred partner), and contracting directly with that vendor.