

News from the City of Dearborn

Discover Dearborn! Visit www.WelcomeHomeDearborn.com

John B. O'Reilly, Jr., Mayor

Department of Public Information

Mary Laundroche, Director

313-943-2285

FOR IMMEDIATE RELEASE

August 23, 2007

Dearborn residents warned of scam: fake email claiming to be from local credit union

Beware of all internet "phishing" scams

DEARBORN, Mich. – Dearborn residents should beware of a recent email scam involving fake emails claiming to be from a local credit union.

The email – which is not from the credit union – has a subject line of "Renew Your Account." It claims that the recipient's account with the financial institution has been suspended, and that the recipient must complete an "account update" before the account will be unlocked.

A link to click on is provided for the supposed "account update."

In reality, the email is an example of "phishing" – an internet scam where con artists try to get people to disclose sensitive personal identification and financial information such as your Social Security Number, or bank account or credit card number.

"People should not respond to this email in any way, or to any email claiming to be from a financial institution that asks for this type of information," said Mayor John B. O'Reilly, Jr. "Not even the best internet filtering services – which try to weed out these types of scams and other junk email – can catch all

of them, so it's up to each individual to be his or her best line of defense against con artists.”

Here's some more information about “phishing” scams.

Criminals will send fake emails – sometimes to millions of people – that are designed to appear to come from a bank or business that you have an account with. The message's sole purpose is to gather that sensitive personal identity and financial information described earlier.

Typically, a message will urge you to take action and will provide a link to what appears to be the official website of the bank or business, but the web site is actually bogus.

The email will appear legitimate, usually containing the company's official logo. However, be aware that the text of the emails often contain spelling errors or poor grammar. If you have any suspicions at all about the message, then the message is probably illegitimate.

The best thing to do is to call the company that allegedly sent you the message. However, never use the phone number included in the message, and never click on a link within a suspicious message.

Finally, if you receive an email message that proves to be a “phishing” scam, report the message to the company that the message claims to be from. Doing so makes the company aware of the scam so they can report it to the proper authorities and warn their customers.

For more information about “phishing” scams and steps you can take to avoid becoming a victim of it, visit <http://www.windowsecurity.com/articles/Avoid-Phishing.html>

* * * * *

MEDIA CONTACT: Mary Laundroche or Randy Coble, at (313) 943-2285

phishing scams aug 2007