

January 11, 2010 **Warning: Text Message Scam**

Someone is posing as the Buffalo Metropolitan Federal Credit Union in text messages! They are attempting to get the mobile phone user to call the telephone number provided in these text messages. The fraudster then attempts to get personal account information from the mobile phone user.

DO NOT RESPOND TO THESE TEXT MESSAGES!

The Buffalo Metropolitan Federal Credit Union will never ask a member to provide their personal information to an unsolicited telephone call, text message, fax, letter, e-mail, or Internet advertisement. If you are unsure if something you received is legitimately from the Credit Union, call (716) 847-6960 ext. 238.

Smishing is a phishing attack sent by Short Message Service (SMS). SMS is a service that allows the transmission of text messages between mobile phones and handheld devices. The message includes a link that, when accessed, takes you to a phishing site where you are prompted to download a program—a Trojan horse that may give the criminals access to your personal information.

Tips to safeguard yourself from Smishing:

Never respond to unsolicited e-mails or text messages; especially coming from people or companies that you do not have a relationship with or regarding services for which you have not contracted. Contact the financial institution or merchant via the regular channels you use to communicate with them.

Remember, for privacy and security, financial institutions do not arbitrarily solicit non-public information from you. Typically they would already have information based on the relationship you have previously established with them.

When you are accessing any accounts online, make it a habit to check for the small yellow lock in the bottom right of your screen. If it's unlocked – you are not in a secure area of the Website.

If you receive a Smishing message, and you do want to check your account, disregard the recorded number and contact your financial institution through the customer service phone number on your statement or credit card.

Pay attention to the URL. Fraudsters cannot exactly mimic a company's website URL, but will often insert one letter or symbol to make it appear legitimate.

Keep a record of services you sign up for on your mobile devices. If you receive a Smishing message for a service you don't think you signed up for...you probably didn't. Disregard the message.

When in doubt, do not respond to an email, voicemail or text message regarding an account. Contact your financial institution through regular channels.

If you receive multiple Phishing, Vishing or Smishing messages from a financial institution, bring it to their attention to help them uncover the fraud.