

# Phishing Scam Alert

October 2007

Members and non-members have recently received email that looks like it came from Georgia Power Federal Credit Union. These emails ask you to go to a website through a link within the email. The website may look like Georgia Power Federal Credit Union's website, and there you will be asked to provide your confidential information.

This is called "Phishing" or "Spoofing" and it is the most common type of online fraud. Fraudsters send these Phishing messages to a large list of random email addresses, hoping to reach a few members with the email. The Spoof websites are designed to steal personal and financial information.

**It is very important to remember that Georgia Power Federal Credit Union never asks for personal information through email. We encourage you to notify us when you receive an email that looks like Georgia Power FCU is requesting personal information.**

## How to Identify a Phishing Email Scam

**Fraudulent Emails Ask For Your Personal Information.** They often ask you to follow a link where you are asked to provide personal account information such as your account number, password, Social Security Number, ATM/Debit or Credit Card number, PIN or other information that only you need to know.

**Link to a Website.** The link usually takes you to a website that looks legitimate and the website or login page asks for your confidential information. Remember, Georgia Power Federal Credit Union never asks you through email to follow a link to enter confidential information.

**Urgency.** A typical fraudulent email wants you to take immediate action. Often these emails threaten to close accounts or claim that your information has been compromised. The fraudsters' goal is to make you act quickly without thinking about what you're doing.

**Phishing Scam emails are sometimes very difficult to identify as fraudulent because fraudsters are able to make their emails and websites look legitimate. If you ever have a question or doubt, stop and call the credit union.**

## What to do if you have responded to a Phishing Scam Email

If you suspect someone has important personal information about you that may be used for identity theft/fraud, call us at (800)-360-6362. You can also contact any of the three consumer reporting companies regarding concerns about identity theft/fraud at:

EQUIFAX  
800-525-6285

EXPERIAN  
888-397-3742

TRANS UNION  
800-680-7289

## Special Measures for Phishing Email Scams

In addition to alerting the Credit Union and the agencies listed above, you can take additional steps to stop the illegal use of your information.

**Change Your Home Banking Password** – The multifactor authentication process should keep others from accessing your account through Home Banking. It is still a good idea to change your password, especially if it has been compromised.

**Report Credit and Debit Cards as lost or stolen** – If you entered your card number, personal identification number or expiration date through a link in an email, have us shut down the card and reissue a new one. Call us at 1-800-360-6362 during normal business hours or after hours: Visa Credit 1-800-325-3678 or Visa Debit 1-800-472-3272.

## How Fraudsters Find Email Addresses

Fraudsters use email addresses from publicly available sources or through randomly generated lists. If you receive a fraudulent email that appears to come from Georgia Power Federal Credit Union, this does not mean that your email address, name, or any other information has been taken from Georgia Power Federal Credit Union. These emails are randomly sent to both members and non-members with the hope that some of the emails will actually reach a member. This is why the scam is called "Phishing"-just like fishing, the fraudsters are hoping to "catch" a few numbers from a large group of people.

## Protect Yourself

Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. Emails and Internet pages created by fraudsters may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to represent a secure site. If you did not initiate the communication, you should not provide any information. If you believe the contact may be legitimate, **contact the Credit Union**. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself.