Internet Security Policy

GEFCU wants to take this opportunity to make our members aware of the increasingly common Internet fraud known as "phishing".
The FBI's Internet Fraud Complaint Center reports a steady increase in complaints involving unsolicited e-mails directing consumers to a false "member service" website or directly asking for member information. These scams contribute to a rise in identity theft, credit card fraud, and other Internet-based frauds.
One type of fraud, known as "phishing", involves sending members a seemingly legitimate e-mail request for account information, often under the pretense of asking the member to verify or re-confirm confidential personal information such as account numbers, social security numbers, passwords, and other sensitive information. In the e-mail, the perpetrator uses various means to convince members that they are receiving a legitimate message from someone whom the member may already be doing business with, such as your credit union. Techniques such as a false "FROM" address or the use of seemingly legitimate credit union logos, web links, and graphics may be employed to mislead the member.
After gaining the member's trust, the perpetrator attempts to convince the member to provide personal information, employing false websites designed to convince the member the website is genuine, or simply embedding a form in the e-mail which the member completes. Criminals will take that information from the member and quickly act to gain unauthorized access to financial accounts, or commit identity theft or other illegal acts before the fraud is identified and stopped.
GEFCU does NOT request personal information from members. GEFCU does NOT use third-party links to our website. GEFCU does NOT send e-mails requesting confidential information, and any member encountering this type of request is asked to contact GEFCU immediately.
Your information and your account accessed through Home Banking is authenticated through the Verisign Security Certificate. Transactions through Home Banking are secured by SSL (secure sockets layer) encryption. The validity of the certificate can be verified by clicking on the Verisign seal on the Home Banking sign-on page.

For more information about the risks associated with this type of fraud, you can visit the Federal Trade Commission's website, which includes the following brochures:
"How NOT to Get Hooked by the 'Phishing' Scam"
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
"ID Theft: When Bad Things Happen to Your Good Name"
http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm
Other Resources:
www.usdoj.gov/criminal/fraud/internet/
www.fbi.gov/majcases/fraud/internetschemes.htm
www.fraud.org/tips/internet/
www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm
File a Complaint – Internet Fraud
www.ic3.gov
www.cybercrime.gov/reporting.htm

GEFCU makes every effort to protect your account, your identity, and your privacy. If you have any suggestions or comments, feel free to e-mail GEFCU at mail@gefcu-austin.org.