

**E M A I L
S C A M A L E R T**



“Phishing”—
Theft
disguised as
a request.

**LEARN HOW TO
PROTECT YOURSELF**

IMPORTANT WARNING:

Phishing scams on the rise

“Phishing” is an attempt at identity theft where thieves send emails or text messages to consumers requesting that they “verify” or reveal personal data.

Things you should know

- ! **We never request** personal information through email or text messages
- ! **We never ask** you to “verify” information in an email or text message
- ! **We will never ask** you to click on a link to a “special” website to verify or request personal information

What if the email looks authentic?

To appear genuine, and gain your confidence, “phishing” emails may contain some or all of the following elements:

- An institution’s branded logo
- The institution’s name in the “sent from” line, subject line and/or body of the email
- A recognizable employee name
- A “special” link to a phony website built to extract personal data
- An assurance of encryption for a secure transfer of personal data

Don’t be fooled. Emails containing these elements, requesting your personal information, are more than likely a scam! **Do not reply to them.**

In the event you receive a suspicious email, contact us immediately to confirm the authenticity of the communication and report the suspicious activity.

Financial Stability with Local Roots



For more information call or visit any Florida Credit Union branch

Gainesville (352) 377-4141 | Ocala (352) 237-8222

Lake City (386) 755-4141 | Starke (904) 964-1427



www.flcu.org