GREATER TEXAS CREDIT UNION | AGGIELAND CREDIT UNION

GREAT NEWS!

A PUBLICATION FOR GREATER TEXAS | AGGIELAND CREDIT UNION MEMBERS

QUARTER 3 | 2024

President's Message

In today's digital age, staying vigilant against fraud is more crucial than ever. We want to remind you of some essential precautions to help safeguard your personal and financial information:

What to Do If You Receive Suspicious Communication

If you receive a suspicious call, text message, or email claiming to be from the credit union and asking for sensitive information, here's what you should do:

1. **Hang Up Immediately:** If you receive a suspicious phone call requesting your personal information, hang up right away. Fraudsters often use urgency to pressure you into divulging sensitive data.
2. **Do Not Respond to Suspicious Texts or Emails:** Avoid clicking on links or responding to messages unless you're sure they're from the credit union asking for personal information. These could be phishing attempts designed to steal your details.
3. **Contact Us Directly:** If you're not certain a call or message is from the credit union, call the number on the back of your credit or debit card. This ensures you're speaking directly with a legitimate representative of the credit union.

We will never contact you to ask for your digital banking login, security codes, or personal information such as your account number or social security number.

What You Can Do to Help Protect Yourself

- Never share your personal banking information like your username and password
- Regularly monitor your account in digital banking
- Set up account alerts so you know when money is being deposited, transferred, withdrawn

For more information on protecting yourself from fraud, visit our website and explore our dedicated fraud prevention resources. We're committed to helping you stay secure and informed.

Your safety and security are paramount. By staying alert and following these guidelines, you can help protect yourself from fraud and keep your personal information secure. If you ever have any concerns or need assistance, don't hesitate to contact us. We're here to help!

Sincerely,

H.N.Baker

Howard N. Baker II
President, Chief Executive Officer
Greater Texas | Aggieland Credit Union

Protect Yourself from Fraud

Phone and Email Masking

The Cybercriminal's Tools of the Trade

In the age of digital communication, cybercriminals have an array of sophisticated tools at their disposal to carry out scams, phishing attacks, and malware distribution. Two commonly exploited techniques are phone and email masking. These methods allow bad actors to conceal their true identities and contact information, making it easier to lure unsuspecting victims.

PHONE MASKING

Phone masking, also known as number spoofing, is the practice of disguising the origin of a phone call by displaying a false or misleading caller ID. Cybercriminals leverage this tactic to impersonate legitimate businesses, government agencies, or trusted contacts.

One common phone masking scam is the "one-ring" scheme. Attackers use auto dialers to bombard phone numbers, letting them ring only once before disconnecting. When victims call back the unfamiliar number displayed on their caller ID, they are connected to a premium-rate phone line that can rack up unauthorized charges on their bills.

Similarly, scammers may spoof the phone number of a local business or government office to lend an air of legitimacy to their calls. They might claim to be collecting past-due taxes, verifying account information, or offering a special deal. The goal is to persuade targets to provide sensitive data like Social Security numbers, financial account details, or remote access to their computers.

Savvy cybercriminals can even make their spoofed numbers appear on victims' phones as a familiar, trusted contact like a family member or coworker. This "neighbor spoofing" tactic exploits the natural tendency to trust those close to us.

CONTINUE READING ON NEXT PAGE »

Greater Good Spotlight: Supporting the Arlington Community

Our Arlington team of 7 employees has donated over 68 hours to the community so far this year, through our Greater Good volunteer initiative! Organizations like:

- **Arlington Charities** whose mission is to lead and engage the community in the fight against hunger and poverty: providing help; creating hope.
- **TangoCharities Feed the City** program, a monthly volunteer opportunity where individuals come together at a local venue to make lunches for people in need.
- **Alliance For Children**, Tarrant County's only non-profit organization involved directly in the protection from child abuse through coordinated and teamed investigations with local law enforcement agencies, medical centers and state agencies with a goal to minimize the trauma of the abuse so that children and families can begin to heal.

We are proud of our team supporting organizations that help the community meet their most basic needs and providing hope and resources for children who need it most.

EMAIL MASKING

Just as phone masking obscures the true origin of a call, email masking hides the actual sender of a message. Attackers can easily forge the "from" field in an email to make it seem like it came from a reputable company, organization, or person the recipient knows and trusts.

Phishing scams are a prime example of email masking in action. Cybercriminals craft messages that appear to be from banks, tech support, online retailers, or government agencies, complete with official logos and branding. These emails typically contain a sense of urgency, such as a pending account suspension or a limited-time offer, to pressure recipients into clicking a malicious link or providing login credentials.

Once victims fall for the trick and enter their information on a fraudulent website, the attackers can steal their identities, drain their bank accounts, or install malware on their devices. Email masking makes it much harder for targets to verify the legitimacy of these phishing attempts.

MALWARE DISTRIBUTION

Both phone and email masking play a role in the distribution of malicious software. Cybercriminals can spoof trusted contacts or organizations to trick users into downloading infected files or granting remote access to their systems.

For instance, an attacker might send an email that looks like it's from the victim's boss, asking them to review an important document. The attachment, however, contains malware that can steal sensitive data, hijack the computer, or even spread to the rest of the company's network.

Similarly, scammers may use phone masking to impersonate tech support and claim there is a critical security issue with the victim's computer. They'll then try to convince the target to allow remote access, at which point the attackers can install malware and take control.

PROTECTING AGAINST MASKING ATTACKS

Recognizing the signs of phone and email masking is crucial for safeguarding against these types of scams and cyberattacks. Some red flags include:

- **Unexpected or unfamiliar caller ID information**
- **Urgent requests for sensitive data or immediate action**
- **Emails with generic greetings, poor grammar, or suspicious links/ attachments**
- **Callers who seem evasive or unable to provide details about their organization**

To protect themselves, individuals should be wary of unsolicited communications, verify the legitimacy of any requests, and never provide personal or financial information over the phone or in emails. They should also keep their software up to date and use robust antivirus/anti-malware solutions.

Businesses can further mitigate the risks of phone and email masking by implementing security measures like caller ID authentication, email authentication protocols (SPF, DKIM, DMARC), and employee training on identifying phishing attempts.

Phone and email masking are powerful tools in the cybercriminal's arsenal, enabling scams, phishing attacks, and malware distribution on a massive scale. By understanding these techniques and staying vigilant, individuals and organizations can better defend themselves against the growing threat of identity theft, financial fraud, and system compromises.

For more information on how to protect yourself from fraud, visit our website :

CLICK **HERE** TO READ MORE

Upcoming Holidays

CLOSURE ALERT

All credit union offices will be closed in observance of the following holidays. But fret not— online and mobile banking are here for your 24/7!

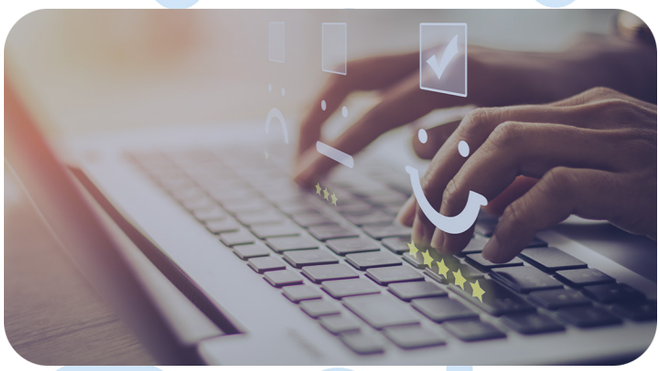
Independence Day
THURSDAY, JULY 4TH

Labor Day
MONDAY, SEPTEMBER 2ND

Find a complete list of holiday closings here:
gtfcu.org/holidays

WE WANT TO HEAR FROM YOU

Take part in our upcoming membership survey via email and share your experience with the credit union



TEX LINE: Your Virtual Phone Assistant

COMING SOON

Available 24/7 to answer your questions and manage your account.

- MONEY TRANSFERS
- BALANCE INQUIRIES
- LOAN PAYMENTS
- AND MORE!

LEARN MORE

GREATER TEXAS CREDIT UNION | AGGIELAND CREDIT UNION