Phishing

Phishing is a fraudulent attempt to obtain your personal information through email or fake Web sites. Here are tips to avoid phishing:

1. Check the sender. If you do not recognize the sender, do not open any attachments, click any links, or reply to the email.
2. Senders can be spoofed, so check the reply address.
3. Know the sender, but was not expecting the email with the attachment? Contact the sender directly and verify they sent you the email.
4. Hover over any links in the email before selecting them. As you hover over a link, the web address will show on the bottom of browser.

Smishing

Smishing is a fraudulent attempt to obtain your personal information through text messages that appear to be from reputable companies. Here are tips to avoid smishing:

1. If you do not know the text sender, do not reply nor select any links within the text message.
2. If you know the sender but the text seems out of the ordinary, call the sender to validate the text.
3. If you receive an app notification via text, do not use the text hyperlink. Go to the app on your phone or the company's website to view the notification.

Vishing

Vishing is the fraudulent attempt to obtain your personal information through phone calls that appear to be from reputable companies, family, or friends. Here are tips to avoid vishing:

1. Trust your instincts. If the call seems out of the ordinary, it probably is.
2. If the caller is pretending to be from a trusted source (friend or company), tell them you will call them back. This way you know the phone number wasn't spoofed.
3. Never give personally identifiable information over the phone. Your credit union will not contact you asking for your social security # or account information.

Tips provided by LMS Consulting