INTERRA CREDIT UNION CAUTIONS PUBLIC REGARDING COVID-19 SCAMS

March 26, 2020| Goshen, Indiana | During these unprecedented times, Interra Credit Union urges the community to be diligent and aware of an increase in fraud and phishing scams as criminals take advantage of the current health crisis, COVID-19. "Criminals will often capitalize on a current crisis to perpetrate a variety of fraud schemes," said Darrin McLaughlin, Senior Vice President of Interra's Information Technology.

"Cybercriminals are often known for taking advantage of current trending topics in the media and utilizing that as prey on consumers," adds Brook Germann, Assistant Vice President of Security and Loss Prevention. COVID-19 is no different and hackers are only getting more creative in their emails, websites and links to hoax individuals. In most cases, these scams contain malicious software that can be added to your computer within seconds if acted upon. This software can take personal information, credit card numbers and even banking credentials.

The Federal Trade Commissions, as well as Interra Credit Union's Information Technology and Security teams, have several tips for you to keep scammers at bay.

- **Hang up on robocalls.** Don't press any numbers and don't say anything. These scammers have been known to pitch scam coronavirus treatments and will try to collect personal information from you.
- **Ignore online offers for COVID-19 test kits or vaccines**. At this time, there are no vaccines, pills or cures regarding COVID-19. There are also no FDA authorized home test kits currently available.
- **The IRS will not contact a taxpayer via email, nor will they send a text message or post on social media.** Scammers will contact you in these outlets requesting account information, passwords and credit card numbers. It's important to ignore and report any communication from these channels to the IRS.
- **Watch out for phishing emails.** These emails can vary and contain misleading information. Some aspects to look out for regarding phishing emails include:
    - **Beware of online requests for personal information.** A coronavirus-based email that seeks personal information such as your Social Security number is a phishing scam.
    - **Check and validate the email address or link.** You can inspect a link by hovering your mouse over the URL to see where it leads. Some links can easily be distinguished as fraudulent, while other times hackers will use links similar to the legitimate source. Recently, hackers have been claiming to be representatives from the WHO (World Health Organization) or the CDC (Centers for Disease Control & Prevention). Don't take the risk and delete the email right away.
    - **Avoid emails that insist you act now**. Phishing emails are often created to provide some sort of urgency or immediate action. The goal is to get you to click on the malicious link and provide personal information… right now. Instead delete the message immediately.

"The key is to stay aware and be alert," stated McLaughlin.

Interra, headquartered in Goshen, was charted in 1932 and has assets of $1.2 billion. The credit union's field of membership spans 18 counties in northern Indiana, with more than 300 full and part-time employees serving nearly 87,000 members. Interra currently operates 15 offices in Elkhart, Kosciusko, LaGrange, Marshall and Noble counties in Indiana and via a suite of robust electronic services at interracu.com.

#

For more information, contact Meegan D. Siegwarth, Vice President of Marketing.
meegans@interracu.com or 574-534-2506 ext. 7159