CREDENTIAL STUFFING AND WAYS TO PROTECT YOURSELF

August 31, 2020 – Consumers are familiar with the term "phishing", as these attacks have been on the cybersecurity radar for quite some time. On the other hand, terms such as "credential stuffing" may not be as familiar. As fraudsters continue their efforts in stealing personal information, they are frequently creating new ways to wreak havoc. Credential stuffing is one of the newest ways hackers are trying cybersecurity attacks in order to accomplish an account takeover. Fraudsters use stolen account credentials typically consisting of lists of usernames and/or email addresses and their corresponding passwords, that often come from merchant compromises, to gain unauthorized access to user accounts through large-scale automated attacks. With these credential stuffing attacks occurring rampantly throughout the nation, it's important to take precautions to keep yourself safe.

"One crucial way to protect yourself from credential stuffing is to create a strong and unique username and password for each of your accounts," stated Brook Germann, Assistant Vice President of Security & Loss Prevention at Interra Credit Union. "It's vital to not use the same password for every account you have as one organization could have stricter security measures in place than another," added Germann. "When the same password is utilized on multiple platforms, it can be significantly easier for fraudsters to track and gather the information they need," he shared. One recommendation is to utilize a password manager which allows the user to securely store and manage their unique username and passwords.

Below are some important guidelines to consider when creating new passwords:

- **Make your password as long as possible.** Acronyms help with long passwords. For example, mh@LLwfaw@s could mean "Mary has a little lamb, with fleece as white as snow."
- **Use numbers and punctuation.** Upper and lowercase letters, numbers and symbols in your password all make it more difficult for hackers to duplicate.
- **Avoid the use of dictionary words or names.** Last names or a common word such as "marshmallow" or "password" should be avoided.
- **Change your password frequently.** Experts suggest updating passwords every 90 days to prevent abuse of a password that may have been obtained illegitimately.
- **Keep it confidential.** Don't write down your password or tell it to anyone. Also, never allow a computer to remember passwords.

As an extra security step, be sure your financial institution utilizes a Multifactor Authentication (MFA) with their platforms. "Our top priority is to keep our members safe against these cyberattacks," stated Brittany Leeper, Interra's Fraud Prevention Manager. "By implementing MFA into our technology services platform, we are better able to achieve that priority," Leeper added.

Creating a strong password is instrumental to your online safety. "It's key to stay alert and take the necessary precautions to protect yourself from these attacks," concluded Germann.

Interra, headquartered in Goshen, was charted in 1932 and has assets of $1.3 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. A 16th office is set to open in LaGrange in early 2021. Interra also serves its members with a suite of robust electronic services at interracu.com.

AMERICAN SHARE INSURANCE Your savings insured to $250,000 per account.
By members' choice, this institution is not federally insured.

interracu.com | 574.534.2506
P.O. Box 727 Goshen, IN 46527

#

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

AMERICAN SHARE INSURANCE Your savings insured to $250,000 per account.
By members' choice, this institution is not federally insured.