Avoiding Scams.

Avoiding banking scams is crucial to protect your financial information and assets. Here are some important steps to help you steer clear of common banking scams:

1. **Stay Informed:** Keep up to date on the latest banking scams and fraud tactics. Banks and law enforcement agencies often issue alerts about new scams. Being informed is your first line of defense.
2. **Verify Contacts:** Be cautious when you receive unsolicited calls, emails, or messages from someone claiming to be your credit union or bank. Verify their identity by contacting your financial institution through their official website or a known service number. Do not use the contact information provided in suspicious messages.
3. **Protect Personal Information:** Never share your personal or financial information, such as your Social Security number, credit union/bank account numbers, or passwords, via phone, email, or text messages unless you initiated the contact and are sure of the recipient's identity.
4. **Use Strong Passwords**: Create strong and unique passwords for your online banking accounts. Use a combination of letters, numbers, and special characters. Enable two-factor authentication for an added layer of security.
5. **Beware of Phishing:** Be cautious of phishing emails or websites that mimic legitimate credit unions/banks. Scammers often send fake emails asking you to click on links that lead to fraudulent sites. Always double-check the website's URL and ensure it's secure (look for "https" and a padlock icon).
6. **Protect Your Devices**: Install and regularly update reputable antivirus software on your computer and mobile devices. Keep your operating systems, browsers, and apps up to date to patch vulnerabilities that scammers can exploit.
7. **Secure Wi-Fi Connections**: When accessing online banking or sensitive accounts, use secure, private Wi-Fi networks, such as a home network, rather than public Wi-Fi networks that may not be secure.
8. **Monitor Your Accounts:** Regularly review your credit union/bank statements and account activity to detect any unauthorized or suspicious transactions. Report any discrepancies to your credit union/bank immediately.
9. **Shred Documents:** Shred or securely dispose of financial documents, receipts, and statements to prevent dumpster divers from accessing your sensitive information.

10. **Be Cautious with ATMs**: Inspect ATMs for skimming devices or hidden cameras before using them. Cover your PIN while entering it, and use ATMs located in well-lit, secure areas.
11. **Educate Yourself:** Educate yourself and your family about common scams and how to recognize them. Encourage open communication about any suspicious banking-related interactions.
12. **Report Suspicious Activity:** If you encounter a potential scam or suspicious activity, report it to your credit union/bank and relevant authorities immediately. This can help prevent others from falling victim to the same scam.

By practicing vigilance, protecting your personal information, and staying informed about the latest scams, you can reduce the risk of falling victim to banking scams and ensure the security of your financial assets.

Remember, UBI Financial Credit Union is local and here for you! Please let us know how we can help with your banking and financial needs! 860-747-4152 or find us at www.UBIFCU.com

120 Woodford Avenue, Plainville, CT 06062 | 363 North Main St., Bristol, CT 06010

Phone:** (860) 747-4152* | ***Plainville Fax:** (860) 793-1121* | ***Bristol Fax:** (860) 585-0644* | Web:** UBIFCU.com*