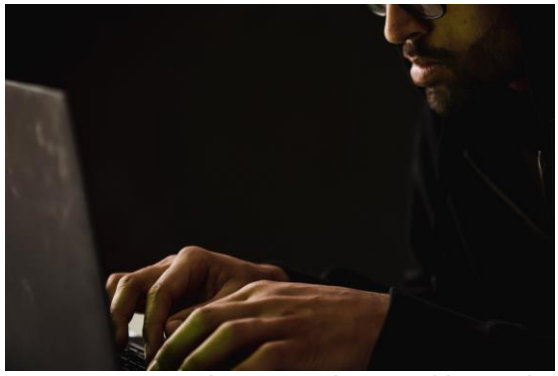

It probably doesn't surprise you to know that scammers are always coming up with creative ways to con people out of their money. Recently, there's been an uptick in an old scam in which crooks reach out to targets and try to gain access to their accounts through micro-deposits. Unfortunately, too many people have already fallen for this scam, and we don't want our members getting caught in the trap. To that end, we've compiled this guide on micro-deposit scams, how they play out and what you can do if you're targeted.

What is a micro-deposit?
Before we can explore the actual scam, it's important to understand how a micro-deposit works.

Micro-deposits are small sums of money transferred online from one financial account to another. The purpose of the deposits is to verify if the account on the receiving end is actually the account the sender intended to reach. Micro-deposits are generally less than $1 and can be as small as $0.02. They are also typically deposited in pairs; within one to three business days of linking accounts, two micro-deposits should appear in your account.

As mentioned, micro-deposits are primarily used to verify account ownership. For example, if you'd like to link your checking account at Franklin First FCU with an investment account, the investment brokerage firm will want to verify that it's sending your dividends to the correct account. Before sending any of your investment earnings, it'll do a test run by sending a pair of micro-deposits to your checking account. You'll be notified that the firm has sent these deposits, and asked to verify the amount of the deposit by logging into your newly linked account. Once you've completed this step, the brokerage account will withdraw the small amount of money sent through the micro-deposits and proceed with regular deposits of investment dividends, as planned.

How the scams play out
Micro-deposit scams can take one of two forms.

In one type of micro-deposit scam, a crook will open as many investment accounts as they can, linking each one to one of a handful of bank accounts. When the micro-deposits begin to come in, the scammer will quickly transfer the money to another account before the brokerage company withdraws the deposits. Though each micro-deposit is small, when multiplied by thousands, the scammer can pull in quite a lot of money — until they get caught, that is.

But it's the other type of micro-deposit scam that concerns us more — and should concern you as well. In this scam, crooks will link brokerage accounts with strings of random numbers, hoping to hit a valid account. When a deposit is verified from an account, they will use additional information about the account holder to withdraw funds from this account as they please. Unfortunately, many people are uninformed about this scam and innocently verify the micro-deposits, giving the scammers free access to their accounts.

Here at Franklin First FCU, we've had an alarming number of micro-deposits made to some of our members' accounts. To protect our members and their money, we've started sending automatic text message alerts to members when they've received a micro-deposit. This way, the member knows about the deposit and, if they don't recognize the sender, they can let us know they've been targeted by a scammer. We can then refuse to let the deposit clear and consider placing a fraud alert on the member's account. Most importantly, the member will know they've been targeted and they can refuse to verify the deposit.

What to do if you're targeted
Micro-deposits are small enough to fly under the radar and you may unknowingly verify one of these deposits with an uninformed click. [However, now that we've initiated our micro-deposit alert system, you will know when to be on the lookout for a micro-deposit and the verification request that follows it.] Here's what to do if you've received a micro-deposit from an unknown source:

Do not verify the deposit. Without verification, the scammer won't know they've hit an authentic account.
Do not click on any links embedded in the verification request message or download any attachments.
Let us know you've been targeted.
Report the scam to the Federal Trade Commission at FTC.gov so they can do their part in catching the scammers.
Let your friends and family know about the scam so they can be on the alert as well.
Scammers are using micro-deposits to gain access to our members' accounts, but Franklin First FCU is doing everything possible to stop them before they can do any real damage. Together, we can beat the scammers at their game and protect your accounts and your money. Stay safe!