

Phishing

Don't Get Hooked - Protect Yourself And Your Identity

The last year has seen a tremendous increase in the amount of identity theft by a technique known as Phishing. Phishing is an Internet based scam where people develop an email campaign or an Internet Website that impersonates a legitimate organization. These people solicit personal and/or financial information from you via email or the Website. This can include Social Security Numbers, account numbers, passwords or PIN's and of course credit/debit card information. The email/website usually implies that there has been a problem or that you are going to lose access to a service if you do not immediately provide the information they are seeking. Other times there is a positive reward if you reply immediately. If you reply to one of these Phishing attempts, you could risk serious financial ramifications. You should never respond to any inquiry asking for this type of information unless you can validate who is asking for it. Phishers generally recreate Websites that are almost identical to sites you are familiar with. Look at the bottom of the browser page for the padlock icon. The locked padlock represents a trusted secured site. If you don't see a locked padlock then you are not actually in our secure HFS site and may be being "phished".

Please be advised Highgrove Community Credit Union will never contact you via email asking for such information. If you receive a suspicious email, please contact us immediately. If you receive a phone call and are not sure it is from the credit union, please ask the person their name and ask them if you can call them back at our regular number.