

## Internet Deception - How to Protect Yourself from Phraud

The technology that we enjoy today, making our lives more entertaining and allowing us to communicate from almost anywhere, also has its risks. Identity thieves have learned how to take advantage of this technology and use it against us, devising numerous ways to obtain personal information they then misuse.

You should be aware of two oddly-named forms of identity theft - phishing and pharming. These are two of the common methods that criminals use to steal your personal information without ever having to touch your wallet or purse.

### Phishing

Phishing is an online form of deception. In phishing scams, someone sends you an e-mail to entice you to provide personal information. They usually try to disguise themselves as legitimate businesses, claiming that they need you to update your account information. They want passwords, credit card information, Social Security Numbers, and bank account information. Typically, they link you to another website to update your information. These websites may look genuine, but they are fake.

TAP FCU will never ask our members to provide confidential account information via e-mail. If you receive an email that appears to be from TAP FCU that asks for personal information, notify us immediately. If you receive something from another financial institution that you do business with, you should also notify them. A reputable business will never send you an email asking you to update your personal account information.

### Pharming

Pharming is a form of identity theft that redirects people from one Internet website to another without their knowledge. Pharmers set up the phony websites to look virtually identical to the legitimate site that the user had intended to visit. The user, thinking the site is the correct one, enters their user name and password, and that information is then captured by the criminals. This gives them access to your account and all the information it contains.

To fight pharming, be observant of the web page address that is shown in the address line. If it seems at all suspicious, do not provide any personal information and close your web browser immediately.

Here are some additional tips to protect yourself from Phishing and Pharming expeditions:

If you get an e-mail or pop-up message that asks for personal or financial information, do not reply and do not click on the link in the message.

- Use computer anti-virus software and a firewall, and keep them up to date.
- Don't email sensitive personal or financial information.
- When providing personal information online, check to be sure that the website is secure, by looking for a lock or key icon at the bottom of the browser.
- Review credit card and bank account statements as soon as you receive them.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.