

Been Phished Lately?

David Dindak
Coast to Coast Data Search
david@2mypi.com

Those dirty little Fraudsters never stop. Identity Theft and Computer Fraud is on a rampage of late. Cybercops are being inundated with reports of Phishers preying on unsuspecting internet users. To prevent you from being one of these innocent victims, here's how it works:

"Phishing" is a term that refers to the on-line imitation of a company in e-mail messages and web sites, created with the intent of fooling unsuspecting users into providing personal information such as passwords, credit card numbers, PINs, etc.

A typical "phishing" e-mail will appear to come from a financial institution like a bank or credit card company. It informs the recipient that some type of problem has affected his/her account, directing the user to follow a provided hyperlink to clear up the problem. The hyperlink leads not to a legitimate site, but to a server (usually in another country where a lot of the people don't even have running water) on which an imitation web site has been set up. The fooled customer is then prompted to enter confidential personal information collected by the scammers for perpetrating identity theft. It then redirects the victim to a legitimate web site to obscure the fact that the individual just gave away data to the bad guys.

Should you encounter any such e-mails, **DO NOT** click on the links or send a reply with any of your personal information. **DELETE THEM!!**

Check with your internet service provider to be certain, but for the most part they would never send out an e-mail asking for personal information. Furthermore, they will not make any changes to mail service without first notifying customers in advance that a change was going to take place, so you know that's a Red Flag from the get-go.

If you ever doubt the validity of an e-mail you received from your banking institution, credit card company or any entity with which you conduct business, contact them with your concern. Report the suspected fraudulent activity, and if your suspicion is correct, contact your service provider so they can take steps at hopefully preventing anyone else from befalling the same fate.

Here is one example of a phishing email:

Hello, _____@XXX.com,

We received your request to reset your XXX.com password. To confirm your request and reset your password, follow the instructions below. Confirming your request helps prevent unauthorized access to your account.

If you didn't request that your password be reset, please follow the instructions below to cancel your request.

CONFIRM REQUEST AND RESET PASSWORD

Click on the following web address: <http://----->
CANCEL PASSWORD RESET

Click on the following web address: <http://----->

Thank you,

Your Banking.com Team

See ya next months.....David