



Important Anti-Phishing Risk Alert: Don't Get Hooked!

Risk Alert

April 2016

www.ciaw.us

Questions?
If you have any questions regarding this risk alert, please contact your local agent, or your Clear Risk Solutions Risk Manager directly at 800.407.2027.

Recently, one of our program members became a victim of an Internet phishing attack. For anyone wondering what this means, phishing is defined as, trying to obtain financial or other confidential/private information from Internet users, typically by sending an e-mail that looks as if it is from a legitimate organization, but contains a link to a "fake" website that replicates the real one. More sophisticated phishing scams might even be disguised as communications from individuals within your entity.

Phishing has been the biggest financial threat on the Internet, but hackers are now going after far more than just financial information; they are targeting government and other large institutions in their attempts.

Phishing attacks can come in different ways:

- E-mail attacks directed at large, unrelated groups of people.
- E-mail attacks directed at smaller, related groups.
- E-mail attacks directed at selected executive level individuals.
- Browser attacks, sometimes called "tab napping" where hackers attempt to lure individuals into opening a tab they have inserted into the victim's browsing session.

We strongly recommend each of our program members review the phishing awareness training that has been provided by the United States Department of Defense at the website below:

http://iatraining.disa.mil/eta/phishing_v2/ph01/module.htm?refresh=1&

Please note: Additional information regarding this topic will be sent, as it becomes available.