Phishing – How Not to Get Hooked

Phishing is a particularly devious form of Internet scam. Customers of banks and financial institutions are often prime targets for “phishers” who trick them into divulging sensitive personal information such as their credit- or debit-card account numbers and personal identification numbers (PINs), by making bogus offers using spoof e-mails and fake Web sites. The technique is also used to steal identities.

One of the reasons phishing is so successful is that the e-mails link the victim to official-looking Web sites where the attackers use images, logos, and text taken from genuine companies’ sites to make the bogus offer appear legitimate.

Phishing is often carried out on a grand scale, targeting hundreds of thousands of consumers at a time—some attacks involve over a million phishing e-mails. Depending on the scam, response levels can be as low as one percent or as high as 20 percent. With the huge numbers involved, the potential financial rewards can be phenomenal.

There are a few simple steps you can take to avoid getting caught by a phishing scam. The most immediate of these is to check that the Web address (the URL) is the same as the real company’s. If it is not, be suspicious and check further before releasing any personal information.

As standard forms of identity verification are unlikely to change in the short term (e.g., Social Security numbers and mother’s maiden name), it will still be necessary to divulge this kind of information. It would be wise to adopt the following rules for protection:

- Use spam detectors to block malicious or fraudulent e-mails
- Use filters to automatically detect and delete malicious software
- Employ software to block outgoing delivery of sensitive information to malicious parties
- Implement good quality anti-virus, filtering, and anti-spam software solutions like McAfee® Internet Security Suite

Businesses can also help to protect their customers by:

- Establishing corporate policies for e-mail content
- Providing a way for customers to validate e-mails
- Establishing strong authentication at Web sites
- Regularly monitoring the Internet for potential phishing Web sites

Phishing differs from traditional scams primarily in the scale of the fraud that can be committed. Awareness is a major first step in prevention.

McAfee
227 Bath Road
Slough, SL1 5PP
United Kingdom
+44.1753.217.500
www.mcafee.com

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red is in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. ® 2008 McAfee, Inc. All Rights Reserved.