

Crime You Can Bank On

The recent collapse of many significant financial institutions is going to bring on a wave of phishing attacks, as well as other more traditional crimes. Part of the reason these crimes will be so successful is due to the confusion that many people will have over their accounts with mergers, acquisitions, and other changes taking place. They will be expecting all kinds of inevitable changes, including filling out forms and other paperwork. This will make trusting individuals more vulnerable to attack.



Randy Abrams

A prime example of an expected attack vector is Washington Mutual. The people who withdrew their money (less than \$100k) from Washington Mutual out of fear, are the confused people who are most likely to be the first wave of crime victims. Some of these people no doubt, resorted to the money-under-the-mattress technique. This facilitates the traditional crime of burglary and is not FDIC insured. If traditional criminals were as savvy as cyber-criminals, they would have been waiting outside of Washington Mutual Bank branches to take the cash from customers as they withdrew their savings and walked out the doors holding ridiculous amounts of currency.

The digital attacks will begin en masse when letters start going out to account holders to advise them of changes once Washington Mutual has been taken over completely. At that time we will see phishing attacks that prey upon confusion.

Washington Mutual is only one example. We will see an increase in attacks on other banks and brokerage accounts as well. Customers of any financial institution that is taken over need to be on high alert for scams advising them to divulge personal information as part of the process.

There will be actions that need to be taken. However in all cases it is advisable to use a phone number from the telephone book, or regular statement to validate such requests. The attacks will come in the form of emails, phone calls and even SMS text messages.

Never use the contact information in these messages. Call your financial institution with a known valid phone number to validate requests for information.

Remember, your name, your address, your social security number, your mother's maiden name, your address, and your telephone numbers are all public information. In many cases your bank account number—especially credit card numbers—may be essentially public information.

No matter how convincing and official a letter or phone call may seem, be sure to call back to a known valid number or you may likely become a non-FDIC insured victim.

If you wish to submit questions or comments to "Ask the Expert" please feel free to send them to askeset@eset.com.



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.