Protect Yourself

How to Recognize a Phishing, Mishing or Vishing Scam

Genuine banks and organizations will NOT contact you by e-mail to request confidential and personal information. If a bank or organization sends you a genuine request for some information, they should address you by name and not refer to you as "account holder" or "customer".

A genuine bank or organization should take good care to ensure that any e-mail or message they send to you does not contain typing errors and grammatical mistakes—many scammers make silly mistakes.

How to Respond to a Phishing, Mishing or Vishing Scam

There are things you can do if you receive a suspicious message. If you receive an e-mail, phone call or other message supposedly from your bank or another organization requesting your personal details, delete the message or hang up your phone. Even if the e-mail or message urges you to act quickly, do not panic—this is just a trick to make you respond immediately without giving you a chance to talk to others or to check if it is a scam.

If you receive a suspicious call or message that you think might be genuine, do not divulge your details until you have made some extra checks to satisfy yourself that it is not a scam.

Ring your bank or the company yourself to find out if it is a genuine message but never use the number provided in the e-mail or message—a scammer will not give you the correct number!

How to Reduce the Damage if You Have Fallen For a Scam

Report the scam - You should telephone your bank or financial institution if you are suspicious of an e-mail, letter or phone call that claims to be from them, or if you think someone may have access to your accounts. They can advise you on what to do next. Make sure the telephone number you use is from the phone book or your account statement, ATM card or credit card. Protect your computer - If you were using your computer when you got scammed, it is possible that a virus of other malicious software may have infected your computer. Run a full system check using reliable security software. If you do not have security software (such as virus scanners and a firewall) installed on your computer, a computer professional can help you choose what you need. Change your passwords - Scammers may have also gained access to your online passwords. Change your passwords using a secure computer.