Best Practices for Cardholders – Bank of America Tips to Keep your Card and Account

Secure **Keep your card and account secure**

1. If your card is lost or stolen, call Bank of America immediately.
2. Report suspicious activity to Bank of America immediately.
3. If the Bank of America fraud team calls you, return the call as soon as possible.
4. If you are suspicious about a caller, hang up and call the number on the back of your card.
5. Never give your card number to someone who calls you.
6. Never send your credit card number, three digit code or expiration date in an e-mail.
7. Once you have contacted Bank of America and received the fraud affidavit, complete and send the affidavit back promptly.

Monitor your account activity

1. Check your transactions against your receipts regularly online or on your statement, and report any unrecognized transactions immediately.

Keep your card safe while shopping online

1. Make sure you are on a secure site when making purchases online – check for the lock icon or verify that the site is https.
2. Do not click on a link to make a purchase. Manually type in the URL yourself.
3. When shopping online, the only information you should be asked by the merchant for are: card number, expiration date, the three or four digit security code and your billing/shipping address.
4. Do not store your information on a website. If asked should the computer remember the information, click "no."
5. Think twice about making purchases when using a public Wi-Fi hotspot. You are safer behind your organization's firewall.

Be aware of Phishing

Phishing is an attempt by fraudsters to gain private information about cardholders and their accounts, such as usernames and passwords, by masquerading as a trustworthy entity in an electronic communication http://en.wikipedia.org/wiki/electronic_communication. There are various methods of phishing such as email, phone calls or text messages which often direct users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

It is **not** Bank of America's practice to send an e-mail or text message:

- that requires you to enter personal information directly into the e-mail
- threatening to close your account if you do not take immediate action of providing personal information
- asking you to reply by sending personal information
  asking you to enter your user ID, password, or account number into an e-mail or secure web page