Cyber Security

Protecting Yourself

Keep Your Computer System Up To Date

- Upgrade or Replace Windows XP Computers
- Keep Your Operating System Up To Date
- Update Your Bios.
- Update Your Email Program
- Update 3rd Party Web Apps Like Flash and Java

Keep Your Web Browser Up To Date

- Dangers of Using an Outdated Browser.
- Most Current Browsers Will Automatically Update
- How to Check If Your Browser is Up To Date

Firewalls

- What is a Firewall.
- Turning on Windows Firewall.
- 3rd Party Firewalls.

Install New Programs Carefully.

- Know What You Are Installing.
- Even Reputable Programs Install Additional Software.
- No One Works for Free.

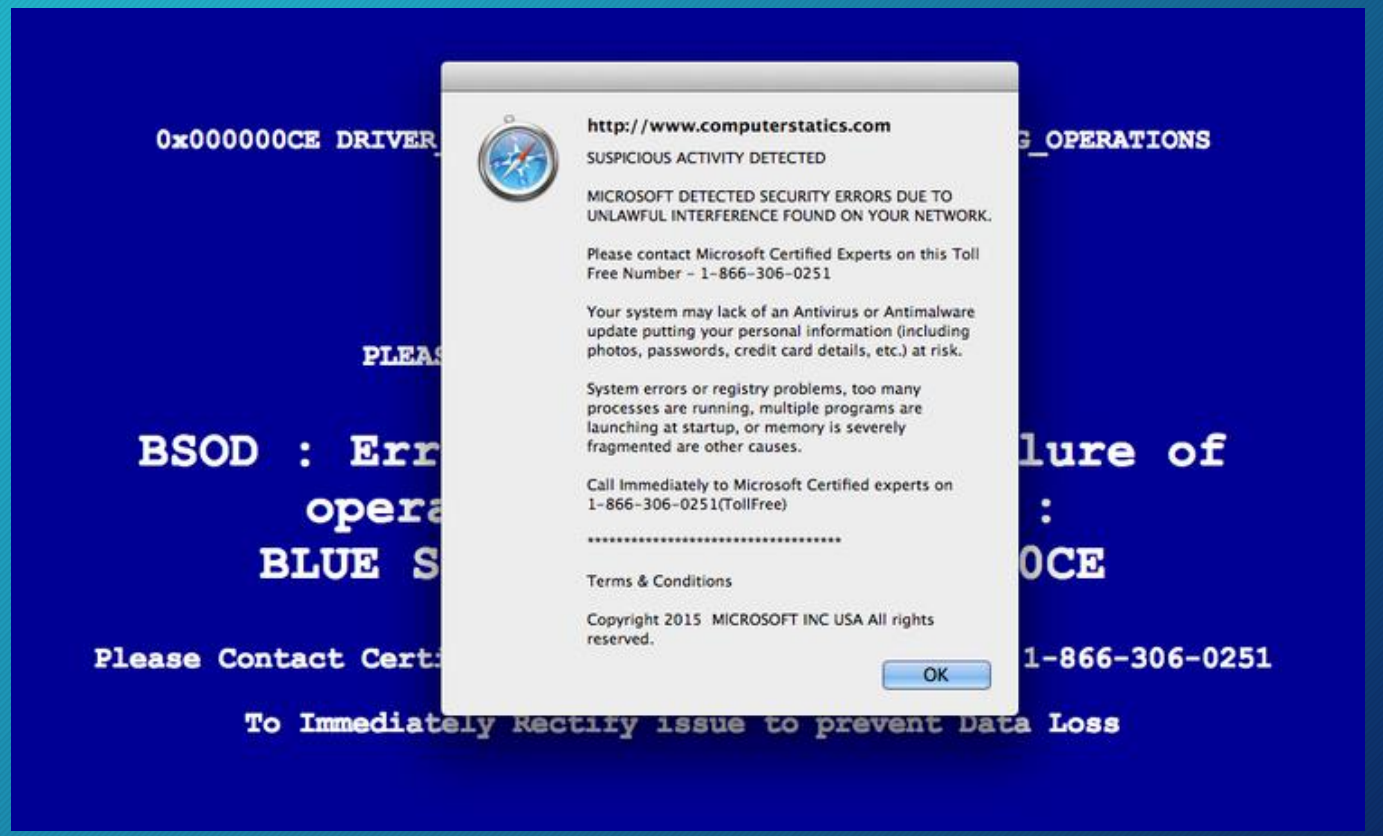
Install New Programs Carefully.

Watch Out For POP Ups.

- Fake Antivirus.
- Fake Browser Updates.
- Registry Cleaners.
- Anything That Pops Up That You Were Not Expecting.

Watch Out For POP Ups.

Watch Out For POP Ups.



Stay Away From Dangerous Sites.

- Adult Sites.
- Torrent or Other Free Software Sites.
- Sites That Stream Unauthorized Movies / TV Shows.
- Gambling Sites.
- Drug Sites.
- Hacking Sites.

Antivirus.

- Windows Built in Antivirus – Windows 10.
- Paid Antivirus.
- Mostly Free Antivirus.
- Open Source Or Free Antivirus.

Passwords.

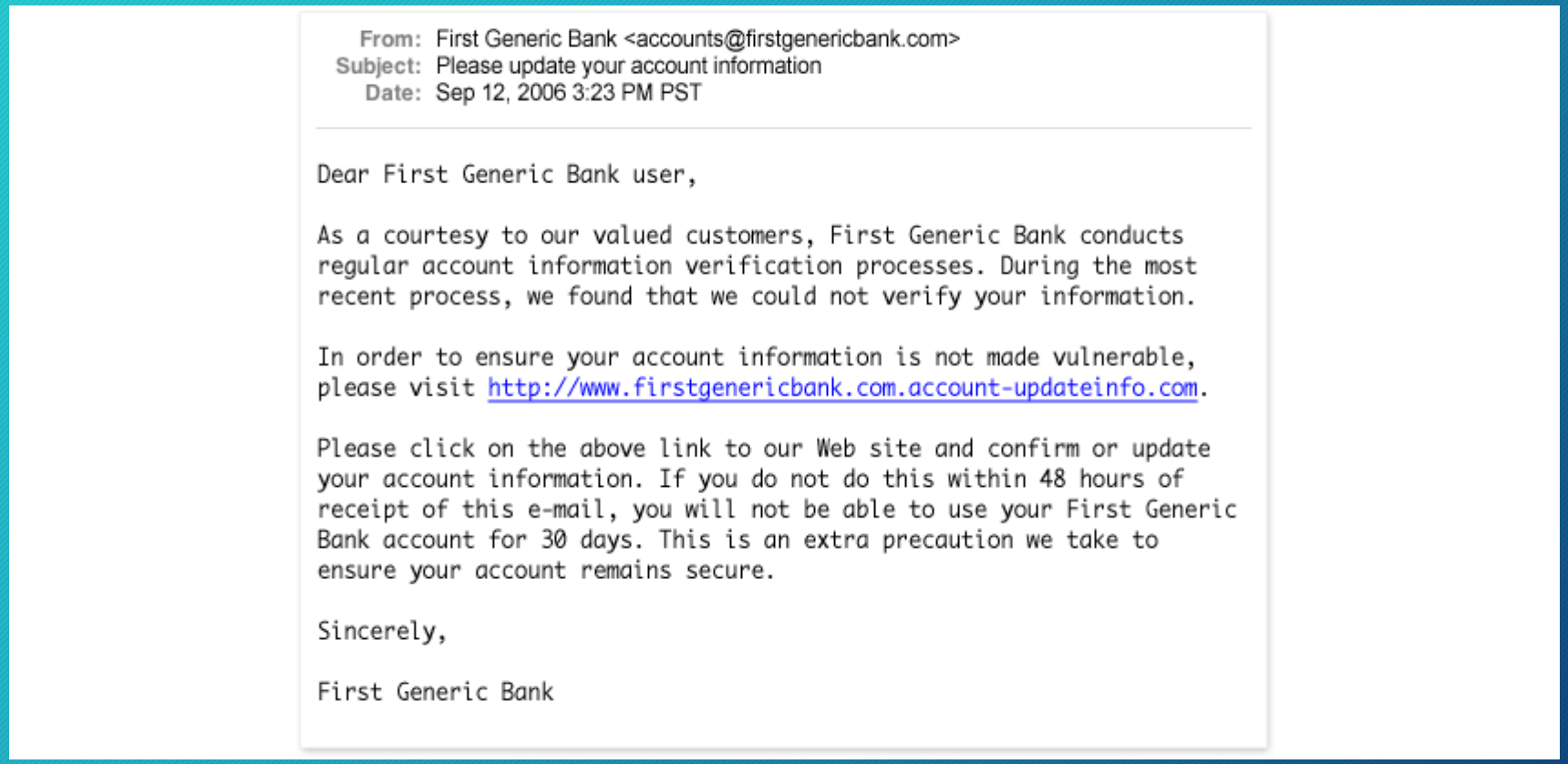
- Use Long Passwords With Caps, Lowercase, Numbers and Spec Characters Don’t Use Words Tied to You or in the Dictionary if You Can Help It.
- Use a Different Password For Every Site.
- Password Vaults.
- Compound Passwords.

Phishing

Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
-Wikipedia

Phishing



From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

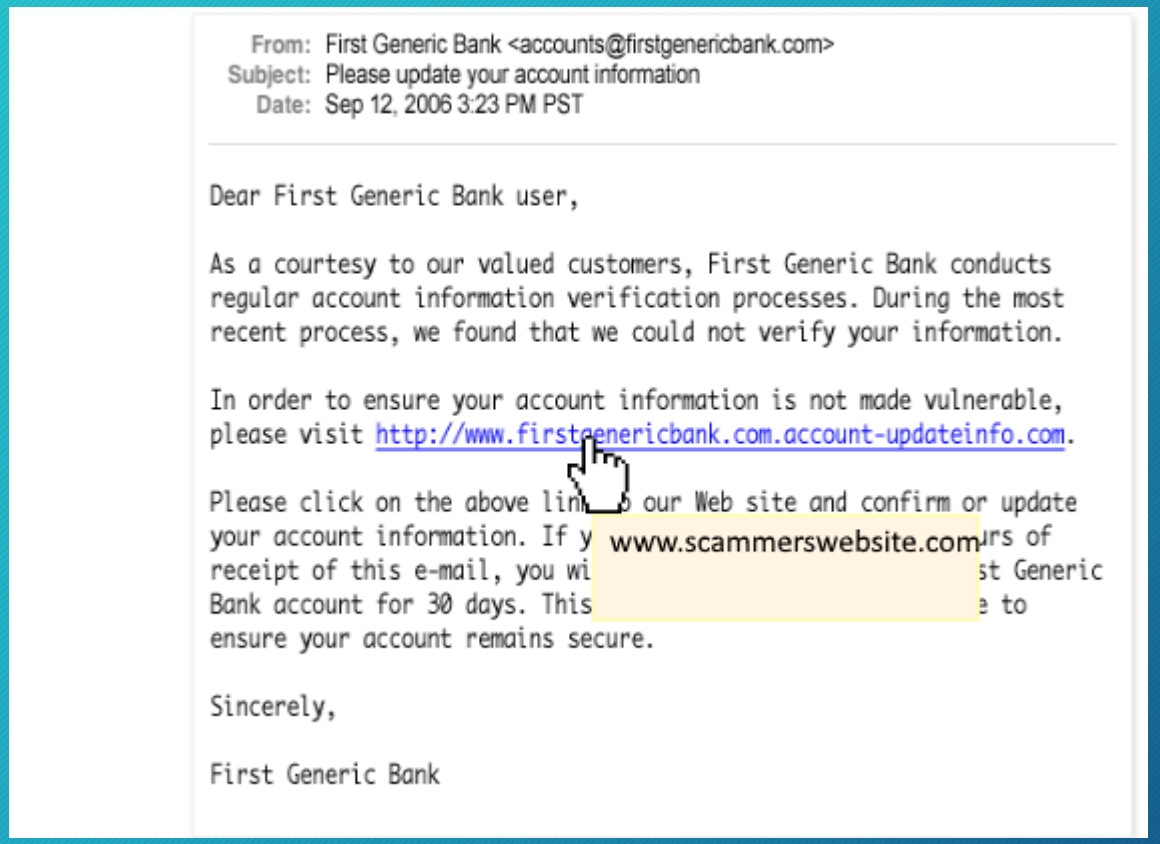
In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank

Phishing



From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

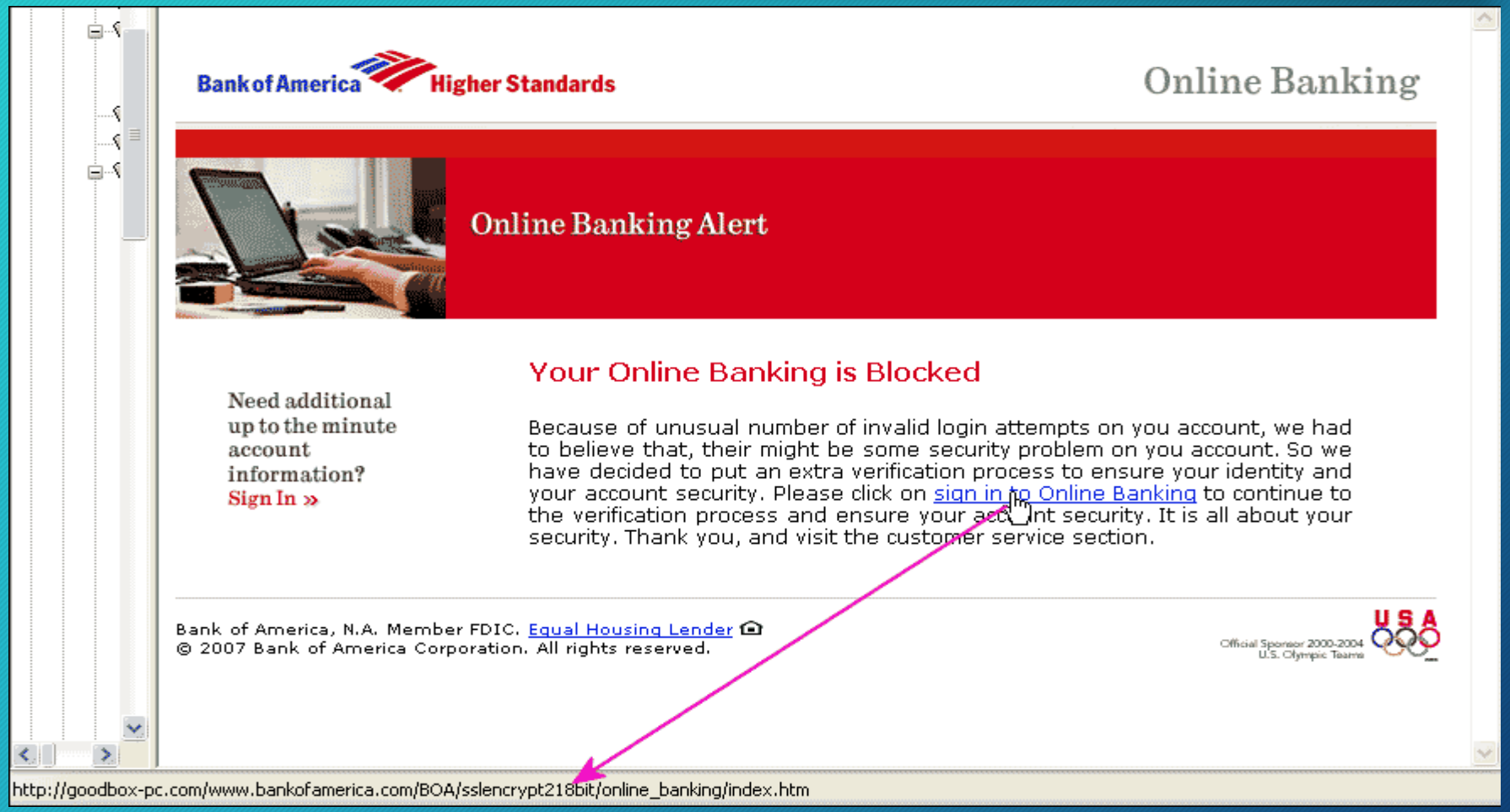
Please click on the above lin[illegible] our Web site and confirm or update your account information. If y[illegible]urs of receipt of this e-mail, you wi[illegible]st Generic Bank account for 30 days. This[illegible]e to ensure your account remains secure.

www.scammerswebsite.com

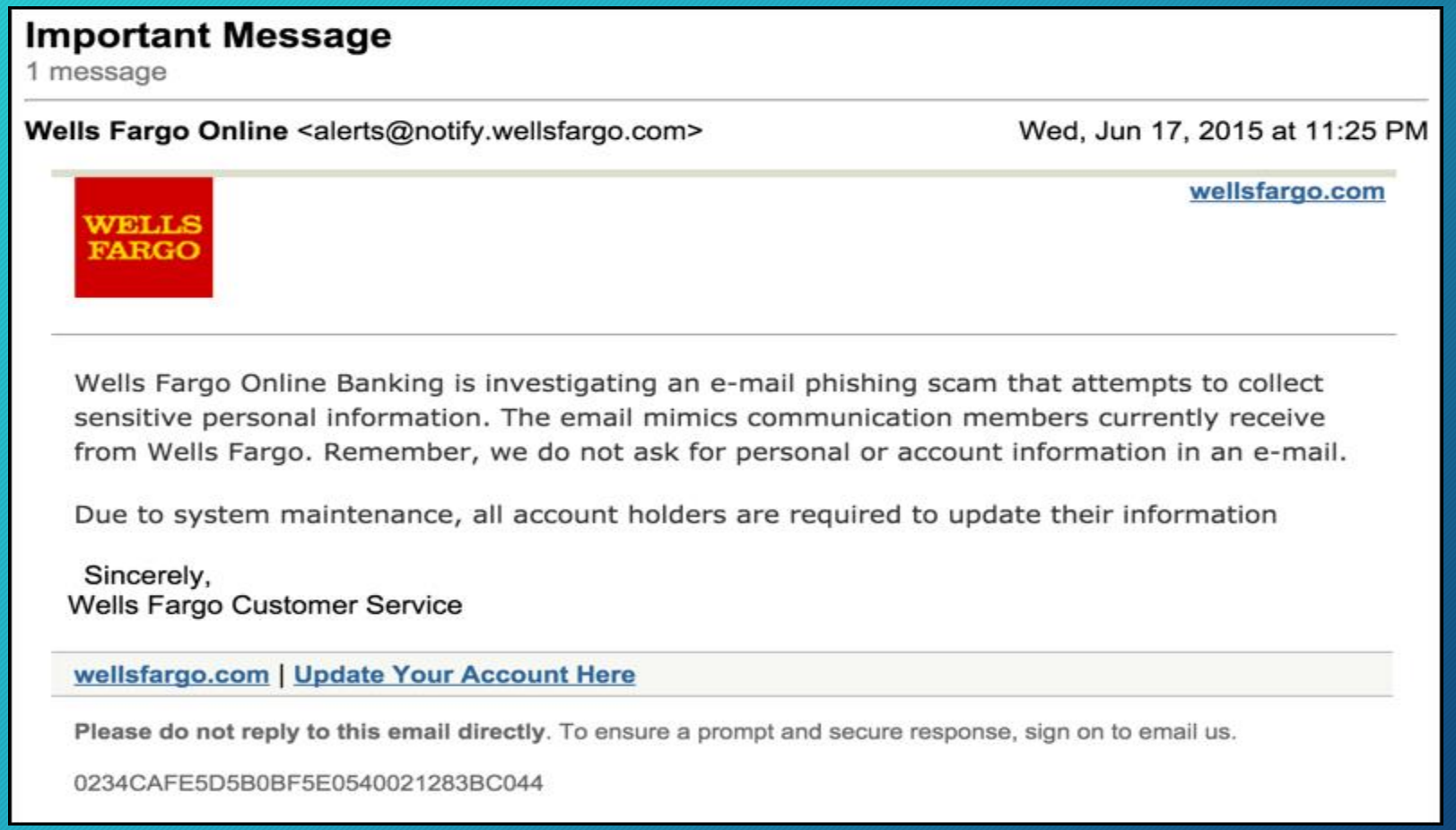
Sincerely,

First Generic Bank

Phishing


Bank of America
Higher Standards
Online Banking
Online Banking Alert
Need additional up to the minute account information?
Sign In »
Your Online Banking is Blocked
Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you, and visit the customer service section.
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2007 Bank of America Corporation. All rights reserved.
USA
http://goodbox-pc.com/www.bankofamerica.com/BOA/sslencrypt218bit/online_banking/index.htm

Phishing



Important Message
1 message

Wells Fargo Online <alerts@notify.wellsfargo.com> Wed, Jun 17, 2015 at 11:25 PM

WELLS FARGO

wellsfargo.com

Wells Fargo Online Banking is investigating an e-mail phishing scam that attempts to collect sensitive personal information. The email mimics communication members currently receive from Wells Fargo. Remember, we do not ask for personal or account information in an e-mail.

Due to system maintenance, all account holders are required to update their information

Sincerely,
Wells Fargo Customer Service

wellsfargo.com | Update Your Account Here

Please do not reply to this email directly. To ensure a prompt and secure response, sign on to email us.

0234CAFE5D5B0BF5E0540021283BC044

Phishing


Phishing Detected!
http://www.facebook.com/home.php
Warning: Suspected phishing site!
The website at static.ak.fbcdn.net has been reported as a "phishing" site.
Phishing sites trick users into disclosing personal or financial information, often by pretending to represent trusted institutions, such as banks.
Learn more about phishing scams.
Proceed anyway
Back to safety
Report an error

More

- Never Use Links in Emails
- Don’t Sent Money via Western Union.
- Don’t Give Info To People You Don’t Know, Call First.
- Don’t Open File Attachments.

Phishing

USE GOOGLE!