

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.



A screenshot of a Firefox browser window displaying the Adobe Flash Player download page. The address bar shows 'get.adobe.com/flashplayer/'. The page features the Adobe logo and navigation links. The main content area displays 'Adobe Flash Player 11.8.800.94 (16.9 MB)' and identifies the user's system as 'Windows 64-bit, English, Firefox'. A prominent 'Download now' button is visible at the bottom. A McAfee Security Scan Plus advertisement is also present, with a checkbox for 'Yes, install McAfee Security Scan Plus - optional (0.9 MB)' which is checked.



A screenshot of the Java Setup window. The title bar reads 'Java Setup'. The window features the Java logo and the Oracle logo. The main heading is 'Offer to Install the FREE Browser Add-on from Ask'. Below this is a search bar with the Ask logo and a 'Search' button. A list of three checkboxes is shown, all of which are checked: 'Install the Ask Toolbar in Google Chrome', 'Set and keep Ask as my default search provider', and 'Set and keep Ask.com as my browser home page and new tabs page'. A red arrow points to the first checkbox. At the bottom, there are 'Cancel' and 'Next >' buttons. A disclaimer at the bottom states: 'By installing this toolbar and associated updater from Ask.com, your use is subject to the Ask.com Terms and Conditions and Privacy Policy. The Ask Toolbar is a product of APN, LLC.'

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.

Attention! Threats found

Attention! 22 threats found!

E-Set Antivirus

File Name	Threat	Alert level	Status
📁 Email-Worm.Zhelatin	Critical	Remove	Active
📁 Backdoor.POISON.BQA	Medium	Quarantine	Active
📁 Spyware.BANKER.ID	Low	Fix	Active
📁 Backdoor.POISON.BQA	Medium	Quarantine	Active
📁 Keylogger.iSnake.PRO	High	Remove	Active
📁 Trojan.Injector.BZ	Medium	Quarantine	Active

Threat name: Email-Worm.Zhelatin
Alert level: 
Action: Remove this software immediately
Infected file: C:\CONFIG.SYS
Description: Worm Email-Worm.Zhelatin.vy is virus-like malware with destructive code, and is able to mutate, replacing its own code by itself. This makes Email-Worm.Zhelatin.vy very dangerous, hard to find, and difficult to delete. Like most viruses, worm Email-Worm.Zhelatin.vy may spread to the other computers by secretly emailing themselves to Internet users in your address book.

Recommended: Please click "Remove All" button to heal all infected files and protect your PC

Remove All

Watch Out For POP Ups.

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:

To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.




0x000000CE DRIVER

PLEASE

BSOD : Error
oper
BLUE S

Please Contact Cert

To Immediately Rectify Issue to prevent Data Loss

<http://www.computerstatics.com>
SUSPICIOUS ACTIVITY DETECTED

MICROSOFT DETECTED SECURITY ERRORS DUE TO UNLAWFUL INTERFERENCE FOUND ON YOUR NETWORK.

Please contact Microsoft Certified Experts on this Toll Free Number - 1-866-306-0251

Your system may lack of an Antivirus or Antimalware update putting your personal information (including photos, passwords, credit card details, etc.) at risk.

System errors or registry problems, too many processes are running, multiple programs are launching at startup, or memory is severely fragmented are other causes.

Call Immediately to Microsoft Certified experts on 1-866-306-0251(TollFree)

Terms & Conditions

Copyright 2015 MICROSOFT INC USA All rights reserved.

OPERATIONS

ture of

:
CE

1-866-306-0251

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


Bank of America Higher Standards Online Banking


 **Online Banking Alert**

Your Online Banking is Blocked

Need additional up to the minute account information? [Sign In >>](#)

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.


Official Sponsor 2000-2004
U.S. Olympic Teams 

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

 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



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!