Guidelines for Software Applications
Ver. 2.0

Overview

StopBadware provides tools and information that assist industry and policymakers in meeting their responsibility to protect users from badware, and that help users protect themselves. This document is one such tool. It represents a **minimum** set of guidelines for software behavior that we believe all applications should meet or exceed. Applications that fail to meet these guidelines may be considered badware—software that fundamentally disregards users' choices about how their computer or network connections are used.

These guidelines were developed by StopBadware in consultation with software industry representatives, privacy advocates, security experts, lawyers, and other members of the Internet community.

Definitions

User: a person authorized by the owner of a computer or network to operate the computer or communicate using the network

Computer: any electronic device, such as a personal computer or smart phone, that provides the user the ability to install additional or modified software or firmware

Network: any system, such as a local area network or a cable modem connection to an Internet service provider, that allows computers to communicate directly with other computers and/or Internet devices

Administrator: a person authorized by the owner of a computer or network to install software on the computer or to change the configuration of the computer or network

Clearly and conspicuously disclose: make information known in a way that the target individual can reasonably be expected to encounter and understand in the course of his/her normal activity

Guideline 1: Installation

Software must be installed or executed on a computer only with the informed, affirmative consent of the user or administrator.

An application must, prior to installation or execution, clearly and conspicuously

disclose to the user or administrator:

A. that the application will be installed or executed;

B. the name, purpose, and significant features of the application; and

C. the name, purpose, and significant features of any additional applications (including toolbars, plug-ins, etc.) that will be installed by the application or its installer.

The user or administrator must affirmatively consent to the installation or execution of the application.

Notes

1. Applets that execute automatically within a client application in response to a user action (e.g., visiting a website), and in accordance with the user's settings and the intended use of the client (e.g., Java or Flash Player), are not subject to this guideline.

2. Executing an application automatically on a schedule, on system startup, or in response to a trigger does not require disclosure **if** the initial installation is consistent with this guideline **and** the automatic execution is predictable given the disclosed features of the application.

Guideline 2: Potentially unwanted behavior

Software must inform the user or administrator prior to engaging in potentially unwanted behavior.

An application must clearly and conspicuously disclose to the user or administrator any behavior that could predictably be expected to threaten:

A. the security or privacy of the user, the computer, or the network;

B. the operation of other hardware and software on the computer and network;

C. the ability of the user to operate the computer and communicate on the network as the user intends; or

D. the security, privacy, or intended use of remote computers or networks.

The application must give the user or administrator an opportunity to prevent such behavior, whether by opting out of the behavior, closing the application, declining to install the application, or removing the application.

Notes

1. In the case of the transmission or collection of personally identifying information or of data that could be used to profile the user (e.g., web search or browsing history), a detailed explanation of how the data will be used and with whom it will be shared should be readily available to the user in a privacy policy or similar form.
2. Examples of potentially unwanted behavior can be found in appendix A.

Guideline 3: Deceptive behavior

Software must not use deceptive behavior or language to influence decisions by the user or administrator.

An application must not use deceptive behavior or language to induce the user or administrator to:

A. pay or transfer money to any party;

B. install potentially unwanted software on a computer;

C. share private or personally identifiable information with any party; or

D. take any other action that threatens the security or privacy of any computer, network, or user, or the intended use of any computer or network.

Notes

1. Examples of deceptive behavior can be found in Appendix B.

Guideline 4: Removal

Software must provide the ability for the application and all of its functionality to be removed in a reasonable manner and without undue interference.

Uninstalling or preventing future execution of the application and any bundled applications, or stopping their potentially unwanted behaviors, must not require the user or administrator to:

A. possess specialized knowledge that is out of proportion to that required to install and use the application;

B. install additional software;

C. pay a fee to any party;

D. provide personally identifying or private information to any party; or

E. navigate excessive obstacles to the removal process.

Notes

1. Incidental files or settings that are left behind during removal and do not substantively affect functionality of the computer or network are not subject to this guideline.

Appendix A: Potentially Unwanted Behaviors

This extensive, but not exhaustive, list of examples is intended to aid in identifying behaviors that should be clearly and conspicuously disclosed under Guideline 2 and removed under Guideline 4.

- Tampering with settings that affect the user experience, such as the browser's default home page or search engine
- Using data about a user's behavior (e.g., browsing or search history) in ways other than what the user might reasonably expect
- Making personally identifiable information available to someone other than the user or administrator
- Tampering with security or privacy settings
- Sending bulk e-mail (e.g., spam)
- Scanning or attacking remote computers or networks
- Enabling remote control of the local computer or network
- Modifying or providing remote access to documents or other data in a manner unrelated to the disclosed purpose(s) of the application
- Transmitting or providing remote access to a user's keystrokes, screen captures of the user's operation of the computer, or captured network traffic
- Removing, disabling, or changing the functionality of other software
- Adding toolbars or other new functionality to the web browser or other software
- Introducing frequent or persistent advertisements, pop-ups, prompts, or other distractions
- Remapping keyboard, mouse, or other inputs
- Tampering with network settings or traffic (e.g., changing DNS server address or intercepting DNS lookups)
- Introducing self-replicating code (worm, virus, mass mailer)
- Consuming bandwidth by serving data (e.g., via a peer-to-peer network) to other computers not associated with the user

Appendix B: Deceptive Behaviors

This extensive, but not exhaustive, list of examples is intended to aid in identifying behaviors that should be avoided under Guideline 3.

- Disguising an application as a different application or system utility
- Modifying or overlaying web (or similar) content in a way that hides the source or presence of the modifications
- Hiding the presence of the application from the user, administrator, and/or system tools
- Providing a user or administrator with a false choice, or systematically ignoring the user's or administrator's choice
- Exaggerating or grossly misrepresenting the presence of potential threats found on the computer or network
- Communicating that the application has features that it does not have
- Exaggerating or grossly misrepresenting the risk associated with removing, failing to install, or failing to upgrade an application or purchase a service
- Using branding that duplicates or closely mimics a trusted brand that is not associated with the application
- Actively resisting or ignoring reasonable efforts by the user or administrator to end the application's execution