BlackBerry Internet Service

Security Feature Overview

Version: 4.0

BlackBerry

Contents

Overview

The BlackBerry® Internet Service is designed to provide you with automatic delivery of email messages, mobile access to attachments, and convenient access to Internet content.

The BlackBerry Internet Service uses the security of the wireless network that it connects to. Email messages that are sent between the BlackBerry Internet Service and your BlackBerry device are not encrypted. However, email messages that are sent between the BlackBerry Internet Service and your messaging server can be encrypted using SSL encryption. SSL encryption can also be used by the BlackBerry® Browser and other applications on your BlackBerry device to help protect your data when you connect to the Internet (for example, while shopping and banking online). You can also set up your BlackBerry device to help protect it from theft, viruses, and spyware.

Security features

Browsing

Your BlackBerry® device uses SSL encryption to create a highly secure connection to shopping web sites and banking web sites. SSL is the standard encryption protocol that is used in many online banking transactions, ecommerce transactions, and other wireless transactions on mobile devices and computers. Using a highly secure connection helps to protect you against identity theft and unauthorized use of your financial data.

You can determine whether SSL encryption is helping to protect data that you send or receive using the BlackBerry Browser. When your connection uses SSL encryption, a closed lock icon appears in the upper-right corner of the browser screen. When your connection does not use SSL encryption, an open lock icon appears.

Email messages and instant messages

Email messages and instant messages that are sent between the BlackBerry® Internet Service and your BlackBerry device use the security features of the wireless network. Messages that are sent between your messaging server and the BlackBerry Internet Service are automatically encrypted if the server supports SSL encryption.

Attachments

Your BlackBerry® device does not run applications that you receive as attachments in email messages. The BlackBerry® Internet Service processes attachments and renders them in a format that is designed to protect you from potentially damaging attachment code such as macros.

To protect the received attachments that your BlackBerry device stores, you can turn on the content protection feature.

Related information

Encrypting your BlackBerry device data, 5

BlackBerry device firewall

You can set up the built-in firewall on your BlackBerry® device to block incoming SMS text messages and PIN messages, both of which are not encrypted. If your messaging servers support SSL encryption, you can make sure that you only receive messages that are protected by SSL encryption on your BlackBerry device by blocking incoming SMS text messages and PIN messages.

Spam email messages

The BlackBerry® Internet Service has an anti-spam system that is designed to block spam email messages that are sent to your BlackBerry email address. This feature helps to protect you against the inconvenience and potential privacy threat of email messages that are not intended specifically for you.

For additional control of spam email messages, you can create email message filters to prevent unwanted email messages from being delivered to your BlackBerry device.

Encryption of login information

When you log in to the BlackBerry® Internet Service web site using a browser on your computer, the BlackBerry Internet Service uses SSL encryption to help protect your login information and any changes you make to your login information. This encryption is designed to protect your user names, passwords, and other BlackBerry Internet Service account information from unauthorized access.

Security options

Using passwords

You can set a password to help protect your BlackBerry® device from unauthorized use.

You can also use the password keeper to store all of the passwords that you use to access applications and web sites on your BlackBerry device. You need to remember only the password keeper password to retrieve all of your stored passwords.

Encrypting your BlackBerry device data

When you set up encryption of your BlackBerry® device data using the content protection feature, your BlackBerry device is designed to be protected against users with malicious intent who could attempt to steal your data directly from the internal hardware. No one can read your encrypted data without your device password.

In the Security Options, you can set the Content Protection Strength level. The BlackBerry device then encrypts your data (for example, messages, contact entries, and tasks). The Content Protection Strength level optimizes either the encryption strength or the decryption time. When your BlackBerry device decrypts a message that it received while locked, the BlackBerry device uses an encryption key. More encryption strength means a longer decryption process.

If you set the content protection strength to Stronger, use a minimum length of 12 characters for the BlackBerry device password. If you set the content protection strength to Strongest, use a minimum length of 21 characters. These password lengths maximize the encryption strength that these settings are designed to provide.

Encrypting your media card data

Your BlackBerry® device is designed to encrypt media data that you store on a media card according to the Encrypt Media Files field in the Memory section of the device options.

This encryption does not apply to files that you manually transfer to a media card (for example, from a storage device using mass storage mode).

When you store a file on a media card for the first time after you turn on mass storage mode, the BlackBerry device decrypts the encryption key for the external memory file and uses it to automatically encrypt the stored file.

For more information about encrypting media card data, visit www.blackberry.com/support to read article KB16088.

Protecting your GPS location information

Your BlackBerry® device stores GPS location information. Third-party applications and preloaded BlackBerry device applications that support location-based services can use that GPS location information. For example, you can use BlackBerry® Maps to get the GPS location of your BlackBerry device. However, third-party applications cannot access your GPS location information automatically.

When applications have access to your GPS location information, they could potentially track your location or report your location back to a server. To prevent applications from using the GPS location of your BlackBerry device, perform any of the following actions:

- Block specific third-party applications from using the GPS location information.
- Block all third-party applications from using location-based services.
- Turn off GPS technology on your BlackBerry device.
- Delete the BlackBerry Maps application from your BlackBerry device.

Controlling your downloaded applications

You can download third-party applications for your BlackBerry® device over the wireless network by using the BlackBerry® Browser. A third-party application can communicate and share data with other third-party applications and BlackBerry device applications. Third-party applications can also access your calendar entries, email messages, and contacts.

BlackBerry device applications include inherent virus protection and spyware protection that is designed to contain and prevent the spread of viruses and spyware to other applications.

When you download an application, you are prompted to confirm that you trust the source. If you trust the application, the application is installed on your BlackBerry device. You can proactively protect your BlackBerry device from viruses and spyware by only downloading applications from trustworthy sources.

You can use the application controls on your BlackBerry device to prevent the installation of specific third-party applications and to limit the permissions of third-party applications, including the following items:

- resources that third-party applications can access (for example, the messages application, phone application, and BlackBerry device key store)
- types of connections that a third-party application that is running on your BlackBerry device can establish (for example, local connections, internal connections, and external connections)

For more information about changing application controls, see the user guide for your BlackBerry device.

Cleaning memory

By default, your BlackBerry® device continually cleans temporary memory to remove sensitive data that is no longer being used.

The BlackBerry device can perform the following additional cleaning actions:

- overwrite memory
- periodically run the memory cleaning application, which causes applications to empty any caches, free memory, and automatically overwrite the freed memory

The BlackBerry device performs additional cleaning actions during any of the following situations:

- you turn on the content protection feature
- a third-party application that you have downloaded registers with the memory cleaning application

You can set the memory cleaning application to run when you insert your BlackBerry device into the holster or when your BlackBerry device remains idle for a specified period of time. You can also manually run the memory cleaning application on your BlackBerry device, run specific registered memory cleaners in the Security Options on your BlackBerry device, and turn on or turn off memory cleaning.

Deleting all BlackBerry device data

Your BlackBerry® device is designed to permanently delete your stored data and application data when you type your BlackBerry device password incorrectly more than 10 times or you click Wipe Handheld (in the Security Options). When you click Wipe Handheld, you can also select the Include third party applications option to remove all third-party applications and application data from your BlackBerry device.

Before you resell your BlackBerry device, consider using one of the preceding methods to delete all of your data so that the person that buys your BlackBerry device cannot access your personal information.

For more information about preparing your BlackBerry device for resale, visit www.blackberry.com/support to read article KB05099.

Glossary

GPS
Global Positioning System

PIN
personal identification number

SSL
Secure Sockets Layer

Provide feedback

To provide feedback on this deliverable, visit www.blackberry.com/docsfeedback.

Legal notice

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR

ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House
36 Station Road

Egham, Surrey TW20 9LF
United Kingdom

Published in Canada