EA USA Online Data Protection Suite

Frequently Asked Questions

TABLE OF CONTENTS

1

ABOUT THE ONLINE DATA PROTECTION SUITE

WHAT IS INCLUDED IN THE ONLINE DATA PROTECTION SUITE?

The Online Data Protection Suite is data and identity theft prevention software designed to protect your personal information while you surf the Internet. It includes two programs: DataScrambler® anti-keylogging software and PhishBlock® anti-phishing software. You can always access information about the product by clicking on the Nationwide logo at the bottom right of your desktop or by clicking on the DataScrambler®. It adds an extra, real-time layer of protection to whatever other anti-virus, anti-spyware or firewall software you have.

WHAT IS THE DATASCRAMBLER®?

The DataScrambler® is anti-keylogging software that is inserted into your browser and shows the actual keystrokes being replaced by alternate keystrokes, providing a visual display of how your information is being continuously protected.
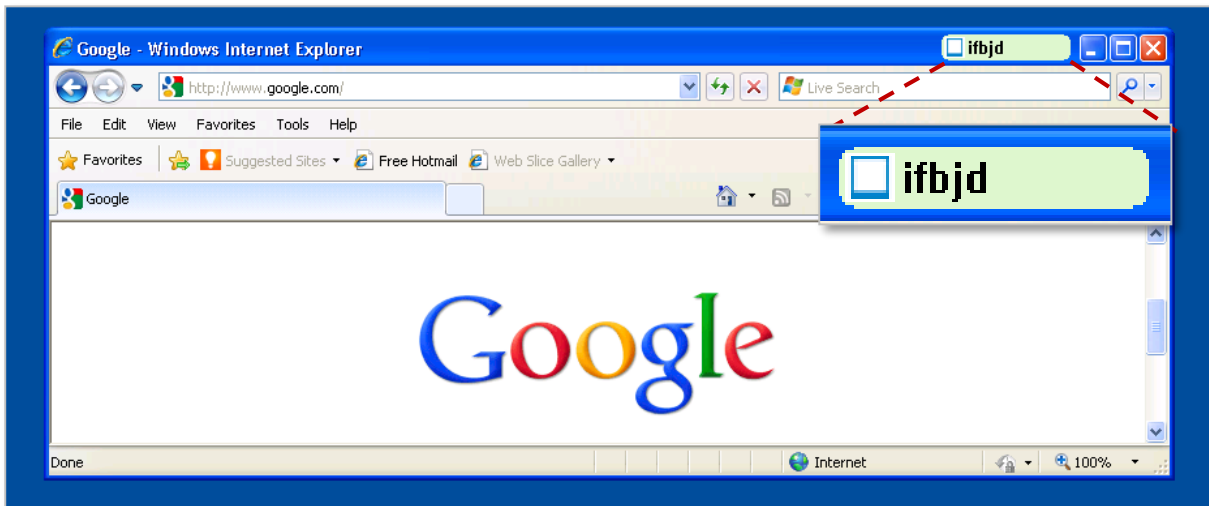
WHAT IS PHISHBLOCK®?

PhishBlock® is anti-phishing software that is proactive and customized; detecting phishing sites the very first time they are loaded. We use proprietary methods to identify phishing sites that attempt to emulate major brands. PhishBlock® can automatically identify a scam site and overlays a warning page to inform you.

3/17/2016

HOW DOES THE ONLINE DATA PROTECTION SUITE COMPARE TO OTHER SECURITY SOFTWARE?

A leading laboratory for the evaluation of security software (West Coast Labs) found the technology behind EA USA's Online Data Protection Suite thwarted a significantly higher number of keylogging and phishing attacks than conventional desktop solutions.

Refer to the chart below for more details on how the Online Data Protection Suite offers additional protection that traditional anti-virus software does not.

BENEFIT	ONLINE & MOBILE DATA PROTECTION SUITE	DESKTOP ANTI-VIRUS, ANTI-SPYWARE OR OTHER INTERNET SECURITY SUITES*
Proactive protection against data entry into all websites	✓	—
Protection without needing to detect and eradicate malware	✓	—
Outperforms all other major desktop security packages in thwarting new spyware attacks	✓	—
Protects against phishing attacks in real-time – outperforming all competitors	✓	—
Plug-and-Play – no configuration required	✓	—
Secure portable browsing on any PC or Flash-based device – USB, mobile phone, etc.	✓	—

*Refers to all major anti-virus products including Norton, McAfee, Kaspersky, AVG and also refers to anti-spyware solutions and combined desktop Internet security suites.

3/17/2016

WHAT ARE THE BENEFITS OF THE ONLINE DATA PROTECTION SUITE?

The Online Data Protection Suite is designed to provide real-time protection against electronic data theft and identity theft, allowing you to browse and use the Internet more safely. This solution is able to prevent illegal and unwanted data capture without needing to identify malware itself. Thus the software provides a complementary, yet more proactive, level of protection than that offered by conventional desktop security solutions.

The Online Data Protection:

- protects every keystroke you type (passwords, credit cards, identity information)

- protects against malware that takes pictures of your data and steals it

- protects you against being lured to a fake (phishing) site that steals your data

- shows every keystroke you type being protected and displays a monthly report showing what data has been protected

To see the protection the software has been providing, view the Activity Report in the software. This can be accessed by clicking on the DataScrambler® or Nationwide logo to bring up the user interface, then selecting the Report tab to view your activity report.

3/17/2016

COMMON TERMS

WHAT IS PHISHING?

Phishing (pronounced "fishing") is a type of online identity theft that involves the use of e-mail and fraudulent websites to steal personal data or information (such as credit card numbers, passwords, account data or other sensitive information).

Con artists typically send millions of fraudulent e-mail messages with links to fraudulent websites that appear to come from brands you trust—such as your bank or credit card company—and request you provide personal information. Criminals can use this information for many different types of fraud, including stealing money from your account, opening new accounts in your name, or obtaining official documents using your identity.

WHAT IS KEYLOGGING?

Keystroke logging, which is often called keylogging, is the action of tracking the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware his or her actions are being monitored. As a generic term, keylogging can also refer to taking pictures of a user's screen to steal data, also known as screen capture.

Keylogging, or a keylogger, is a type of surveillance software or spyware that records every keystroke you make including instant messages, e-mail, and any information you type at any time using your keyboard and then transmits this information to an unknown third party. Those third parties now have access to confidential information such as bank account numbers typed into an online banking site, logins, passwords, etc. Some keyloggers allow not only keyboard keystrokes to be captured but also are often capable of collecting screen captures from the computer.

WHAT IS MALWARE?

Malware, or malicious software, is software designed by criminals to disrupt or deny computer operations, gather information that leads to loss of privacy or exploitation of a user, gain unauthorized access to system resources and/or steal other personal information.

3/17/2016

USING THE ONLINE DATA PROTECTION SUITE

HOW DO I INSTALL THE ONLINE DATA PROTECTION SUITE?

1. Click on the download link available in your program confirmation e-mail.

2. Download the Online Data Protection installation package. Select either 'Run' from the available options or save the file to your desktop and double-click to run the software from there.

3. Follow the instructions/prompts in the software.

4. The installation package will copy the necessary files and license to your computer.

5. At the end of the installation, you will be required to reboot your computer to activate the software.

HOW DO I KNOW IF THE ONLINE DATA PROTECTION SUITE IS WORKING?

If you are running the Online Data Protection Suite, you will see the DataScrambler® located in the top right of your browser, as shown below:

Each time you type into a web page, you will notice that the keystroke you type into a field is replaced by an alternate random character in the DataScrambler®. It is these alternate keystrokes – not what you type – that would be picked up by any hackers trying to monitor your keystrokes.

WHAT HAPPENS IF I GO TO A PHISHING SITE?

If you navigate to a phishing site, your browser will automatically display a warning page to prevent you from entering your personal details. If you choose to, you can ignore the warning and proceed to the site but this is not recommended.

WHICH WEB SITES ARE PROTECTED AGAINST PHISHING?

There are a large number of sites (over 800) that you are automatically protected against, which cover all the main categories of the web such as banking and finance, payment processing, auction sites, utilities, entertainment, social networking sites and more. The list of protected sites is continuously growing and your software will automatically update itself with these new sites.

HOW DO I KNOW WHAT VERSION OF THE SOFTWARE I AM RUNNING?

Go to the Options tab by clicking on the DataScrambler® or double-clicking on the nationwide logo at the bottom right of your desktop and you will see the version number at the bottom of the window.

HOW DO I GET UPDATES FOR THE SOFTWARE?

The software automatically checks each day for new updates. If available, it downloads updates automatically in the background while you use your PC, just like anti-virus software.

WHAT DATA IS TRANSMITTED FROM THE ONLINE DATA PROTECTION SUITE AND MY USE OF IT TO EA OR OTHER PARTIES?

All data submitted from the software (with permission) is anonymous and consists only of counts (e.g. numbers of web sites visited) and profile data (details of operating system, default browser, etc). None of the collected or transmitted data is personal nor is it traceable to an individual user of the software.

CAN I INSTALL THE ONLINE DATA PROTECTION ON MORE THAN ONE PC?

Your license for the Online Data Protection Suite allows you to install the software on up to 3 different computers.

CAN I RE-INSTALL THE ONLINE DATA PROTECTION SUITE AFTER USING UP MY 3 INSTALLATIONS?

You can re-install the Online Data Protection Suite on the same computer as many times as necessary. However, if you have already installed the software on three computers and need to install it on one more machine, you will not be able to complete the installation. The Online Data Protection Suite license allows installation on up to 3 machines only.

HOW DO I UNINSTALL THE ONLINE DATA PROTECTION SOFTWARE?

Go to the Start Menu on your computer, select Control Panel, select Uninstall a Program, highlight the Online Data Protection Suite, then click Uninstall and follow the prompts.

HOW DO I RENEW MY SOFTWARE?

Depending on how you received the software, you may need to renew it once the license expires. You will be prompted by the software to renew near the end of your license period. Just click the renew button and this will automatically take you to the renewal page.

HOW DO I USE THE CREDIT MONITOR TAB?

If you have already enrolled in your credit monitoring service you can enter your policy/member number in the Credit Monitor Tab (accessed from the DataScrambler® or by double-clicking on the Nationwide logo in the tray icon) and proceed to log in to check your credit report. The Credit Monitor Tab also contains your identity theft program's contact information if you ever need support from EA

USA's identity theft resolution specialists about your credit monitoring benefits, your credit report or in case of identity theft.

## WHEN I LOOK AT THE ACTIVITY REPORT IT DOES NOT SHOW MY PERSONAL DATA. HOW DO I CHANGE THIS?

Go to the Options tab (accessed by clicking on the DataScrambler® or double-clicking the Nationwide logo in the tray icon at bottom right of your desktop) and choose the setting to give permission to share your security statistics. Note: only Firefox and Internet Explorer users can receive report data at this time.

I WANT TO TURN OFF MY ACTIVITY REPORT OR SEE IT LESS FREQUENTLY. HOW DO I DO THIS?

Go to the Options tab, accessed by clicking on the DataScrambler® or double-clicking the Nationwide logo in the tray icon at the bottom right of your desktop, and then choose what frequency to display the report. You can also choose "Never" if you prefer to not have the Activity Report automatically appear. In this case, you can still manually access it by clicking on the DataScrambler® or double-clicking the Nationwide logo in the tray icon at the bottom right of your desktop.

I DON'T WANT TO SEE THE DATASCRAMBLER®. CAN I TURN IT OFF?

Yes. To prevent the DataScrambler® from showing within the browser, click on the DataScrambler® (or double-click the Nationwide logo on the tray icon at the bottom right of your desktop), then select the Options tab. The Display Keystroke Substitution option will have a green check mark next to it. Click on the green check mark to change it to a red X. This will disable the DataScrambler® from displaying within your browser the next time you open your browser.
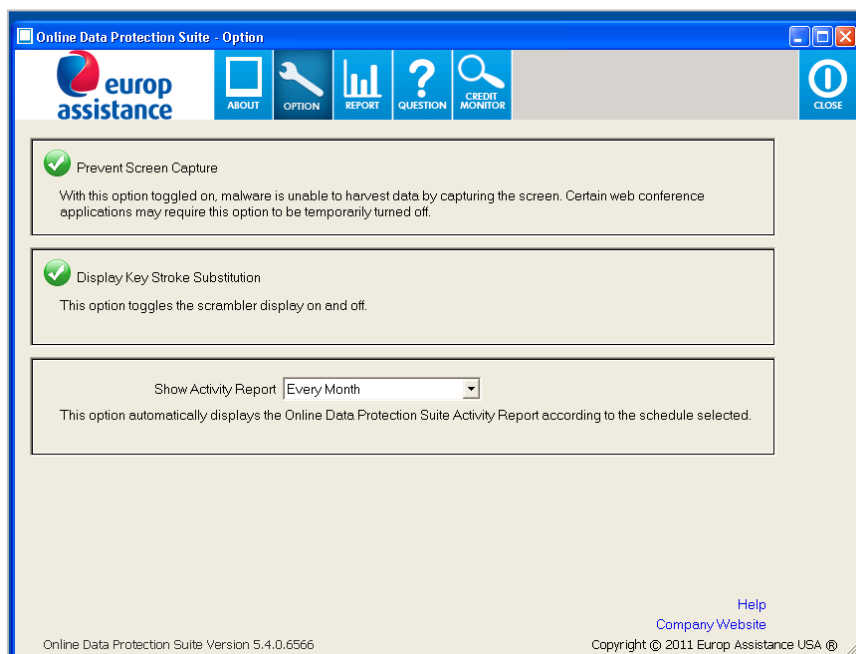
WHAT AM I AGREEING TO BY CHECKING "ALLOW TO PROVIDE ANONYMOUS INFORMATION ABOUT DETECTED THREATS" DURING THE INSTALLATION? WHAT HAPPENS IF I DO NOT SELECT THIS BOX?

When you agree to provide anonymous information about detected threats, this will allow us to collect statistical data that contributes to the Reports Tab section on the malware you are being protected from. This information is statistical and anonymous in nature; no personal information or browsing habits are being collected. If you do not agree to provide anonymous information about detected threats, the Report Tab will not be able to show your statistics.

3/17/2016
Return to Table of Contents
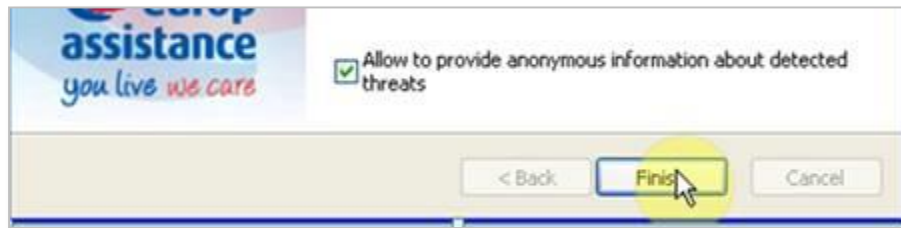
TECHNICAL REQUIREMENTS

WHAT ARE THE MINIMUM SYSTEM REQUIREMENTS TO RUN THE ONLINE DATA PROTECTION SOFTWARE?

The minimum system requirements are:
- Windows XP (SP3), Windows Vista (SP2), Windows 7, Windows 8, Windows 8.1 and Windows 10.
- At least 512 MB RAM, a 233 MHz processor or higher
- 32/64 bit operating system

For browsers, the software supports Internet Explorer 7.0 and above, Firefox 15 and above, and Google Chrome 35 and above.

WHAT INTERNET BROWSERS ARE SUPPORTED?

If you install the Online Data Protection Suite on your PC/laptop, Internet Explorer 7.0 and above, Firefox 15 and above and Google Chrome 35 and above are supported.

WILL THE SOFTWARE WORK WITH MY ANTI-VIRUS OR ANY OTHER SECURITY SOFTWARE?

Yes. The Online Data Protection Suite is designed to work alongside all other security suites and software providing you with an extra, real-time layer of protection against data and identity theft.

DO I NEED ANTI-VIRUS SOFTWARE IF I AM RUNNING THE ONLINE DATA PROTECTION SUITE?

While you now do not need anti-virus to protect against sensitive data being stolen when you use the Internet, anti-virus protects your PC from threats in other areas of your system and has the ability to remove viruses. For this reason we recommend all users install anti-virus and keep it up-to-date.

CAN I USE THE SOFTWARE ON MY APPLE/MAC?

No. The Online Data Protection Suite currently only operates on the Windows operating system. If you have a Windows partition on your Mac, then you can use the software but it is not supported under OS X operating systems.

CAN I INSTALL THE EA USA ONLINE DATA PROTECTION ON MY IPAD OR SMART PHONE?

No. The Online Data Protection was specifically designed for the use on a personal computer. Because your smart phone or iPad runs on a mobile operating system, you will not be able to install the Online Data Protection Suite.

11

TROUBLESHOOTING AND CUSTOMER SUPPORT

I AM HAVING ISSUES USING MY WEB CONFERENCE SERVICE OR SCREEN SHARING SOFTWARE.

While the Online Data Protection Suite supports many such services, the screen capture protection can prevent screen sharing with some solutions. To disable this protection and allow the sharing of your screen, click on the DataScrambler® (or double-click the Nationwide logo at the bottom right of your desktop), then select the Options tab. The Prevent Screen Capture option will have a green check mark next to it. Click on the green check mark to change the option to a red X. This disables the protection. We recommend you restart this protection once you have completed your web conference or screen sharing activity.
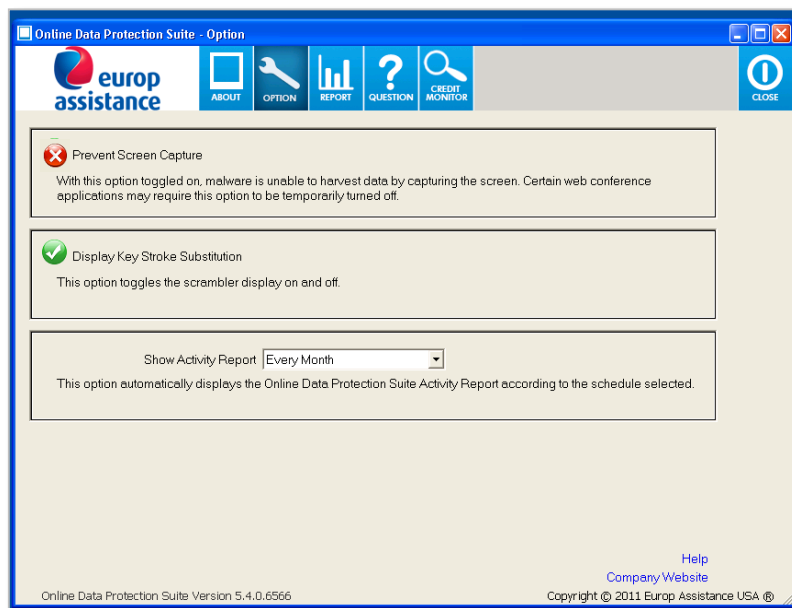

WITHIN CERTAIN WEB PAGES/SERVICES, I HAVE SOME ISSUES USING MY KEYBOARD.

Some services prevent the Online Data Protection Suite key entry protection from working optimally. Restarting your browser or rebooting your computer will generally resolve 99% of these issues.

12

I HAVE A PROBLEM WITH THE SOFTWARE. HOW CAN I GET HELP?

If you are experiencing a technical issue or a problem with the software, you can contact EA by using the Help link located on the Options window of the Report Tab which can be accessed by clicking on the DataScrambler® (or double-clicking the Nationwide logo at the bottom right of your desktop).
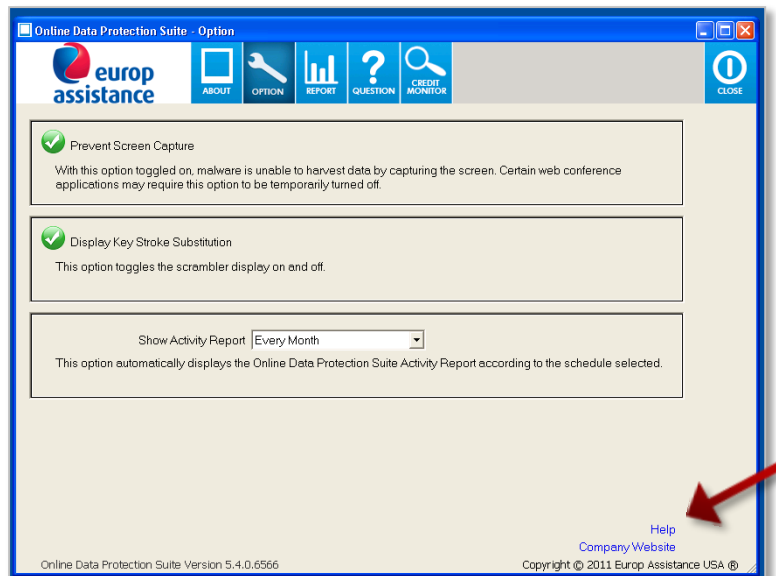
THE ONLINE DATA PROTECTION SUITE FAILS TO INSTALL AND I RECEIVE THIS MESSAGE: "UNABLE TO CONNECT TO LICENSE SERVER. PLEASE CHECK INTERNET CONNECTION."

When the software is unable to connect to the license server, this could mean one of several things. Check the following first:

- Is your computer connected to the Internet?

- Can you open a website via your browser?

- Do you have a local firewall that could be blocking the connection? If so, please disable this for the installation.

Your connection may be blocked if you are located on a corporate LAN or in cases where network firewalls, IDP systems and content scanners exist. You should contact your network administrator for further information.

THE LICENSE FAILS TO VALIDATE DURING INSTALLATION.

If the license fails to validate during installation check the following:

- Is your computer connected to the Internet? For the installation to succeed, an Internet connection is required.
- Do you have a local firewall that could be blocking the connection? If so, please disable this for the installation.

If you are still experiencing a problem, contact EA at DataProtectionSupport@europassistance-usa.com.

13

3/17/2016

I cannot see the DataScrambler®.

If you are unable to see the DataScrambler® located in the top right-hand corner of your Internet browser, check the following:

- Have you installed the Online Data Protection Suite and can you see the Nationwide logo in the top-right hand corner of the browser?
- Did you reboot your computer after installation? If not, please restart your computer as this is a required process to complete the installation.
- Try to minimize and maximize the browser, which sometimes brings the DataScrambler®into focus.
- Try to close and re-open the browser.
- Check to make sure that the browser you are using is supported. View the list of supported browsers
- Check to make sure that the browser is the active application.

I have misplaced my installation file and can no longer find the download link.

If you no longer have the download link, please contact EA at DataProtectionSupport@europassistance-usa.com and we will send you a copy of your confirmation e-mail with the link.

What happens if a warning appears on my computer that refers to the Online Data Protection Suite?

Sometimes you may get a warning screen from your firewall, Windows or anti-virus software about the actions of the Online Data Protection Suite. This is because the software is performing actions needed to protect you that can flag the attention of other software. In most cases you can ignore these warnings and carry on with the use of your computer. The following file names are related to the Online Data Protection Suite:

DPS.exe, EP.exe, Data Protection Suite, PL.exe. If none of these are mentioned in the message, then the message likely does not relate to the software.

If you are ever unsure, you can contact EA customer support by using the Help link located on the Options window of the Report Tab, which can be accessed by clicking on the DataScrambler® (or double-clicking the Nationwide logo at the bottom right of your desktop) or contacting us at DataProtectionSupport@europassistance-usa.com. Please include a screenshot of any warning and a description of the situation in which it arose.

I can't install the online data protection from my gmail account. What should I do?

Sometimes clicking on a link in gmail to open an attachment will open a new window or tab in the browser before starting the download. This sometimes means the download process did not function properly due to your settings in gmail. You should be able to save the file first and then Run it from your downloaded folder. If you are having difficulties saving the file you can right click on the Online Data Protection Suite link in your confirmation email, select Copy Hyperlink and then paste it in a new browser to begin installation. You can also try to turn off popup blocker or add mail.google.com to the allow list. One of these will normally sort out the issue.