

Mediacom Online

Mediacom Online Max

Online Security

- CA Internet Security Suite

- CA ISS - More Information

- **CA ISS - FAQ**

+ General Information

+ Anti-Virus FAQ

+ Anti-Spyware FAQ

+ Personal Firewall FAQ

+ Anti-Spam FAQ

+ Anti-Phishing FAQ

+ Parental Controls FAQ

+ Data Backup FAQ

- CA ISS - Download

Home Networking

Internet FAQ

[To Download a PDF version of this page Click Here](#)

General Information

What does the CA Internet Security Suite Plus 2008 include?

What are the system requirements?

I don't remember my Mediacom email address. What should I do?

After I fill out the registration form what happens next?

What happens if I cancel my Mediacom account?

What happens if I already have security software on my PC?

How does a firewall work?

I think I have a Virus on my PC. What should I do?

Help with License Key?

I have finished downloading, where do I find it?

CA Anti-Virus has detected a Trojan on my computer. What should I do?

What is the difference between the Anti-Spam Folder and the Anti-Spam Folder Quarantine Panel?

Does Anti-Spam automatically delete inbound messages that it considers to be junk email?

Can I use Anti-Spam with my AOL mail?

How does Anti-Spam interact with Outlook rules?

How do I install the firewall?

What if I have more questions regarding this software?

Anti-Virus FAQ

What is a virus?

How do anti-virus products work?

How do viruses spread?

What damage can viruses cause?

What makes CA Anti-Virus different from the rest?

Why does anti-virus software need continually updated signature files?

How does CA Anti-Virus provide automated updates?

How can CA Anti-Virus protect me from tomorrow's viruses today?

Who tests and certifies anti-virus software?

Anti-Spyware FAQ

What is spyware?

How do I get infected with spyware?

Why do I need anti-spyware software?

If I already have anti-virus software, do I need anti-spyware software?

Why not use free anti-spyware software?

Personal Firewall FAQ

What is a firewall?

Why do I need a firewall?

What kinds of threats do firewalls protect against?

If I already have anti-virus and anti-spyware software, do I need a firewall?

Anti-Spam FAQ

What is spam?

Why is spam a problem; can't I just delete spam from my Inbox by hitting Delete?

What kinds of threats does an anti-spam product protect against?

How do I get spam?

Can't I get rid of spam emails by unsubscribing?

How can I solve my spam problem?

Website Inspector (Anti-Phishing) FAQ

What is phishing?

What is the risk in doing business on the Internet?

What are the most common methods of Internet fraud?

What is CA Website Inspector?

What is the CA Toolbar?

What browsers does the CA Toolbar support?

What is the CA Link Advisor?

What applications does Link Advisor support?

Parental Controls FAQ

Why do I need parental controls software?

What are the most common risks to children on the Internet?

How do parental controls products work?

Desktop DNA® Migrator (Data Backup and Transfer) FAQ

What is CA Desktop DNA Migrator?

What is a PC's DNA?

Why do I need a data backup solution?

Why do I need a data migration solution?

What is the difference between a Typical and Custom Migration?

What is the difference between a Deferred and a Real-Time migration?

Can CA Desktop DNA Migrator move a PC's DNA between different versions of applications and Windows operating systems?

Does CA Desktop DNA Migrator migrate Outlook settings and associated mail files?

Download CA Internet Security Suite

[Download Now](#)

What does the CA Internet Security Suite Plus 2008 include?

- **Anti-Virus** - protects against viruses, worms and Trojan horse programs
- **Anti-Spyware** - protects against a wide range of spyware threats
- **Personal Firewall** - stops intruders, blocks malicious programs, and helps protect your personal information
- **Anti-Spam** - makes sure you get messages from people you know, while redirecting messages from people you don't
- **Anti-Phishing** - protects you from phishing attacks, Internet fraud attempts, and malicious websites
- **Parental Controls** - allows you to control and manage Internet access for the whole family
- **Data Backup and Transfer** - helps you backup and restore your important personal data and PC settings, or transfer them to a new PC

[return to top](#) 

What are the system requirements?

- Windows 2000 (SP4+), Windows XP (SP1+), or Windows Vista
- 256 MB RAM (512 MB for Windows Vista)
- 300 MHz or higher processor (800 MHz for Windows Vista)
- Microsoft Internet Explorer 6.0 or higher (7.0 for Windows Vista)
- 150 MB hard disk space
- CD-ROM drive
- Internet access

For Anti-Spam:

- Microsoft Outlook 2000 or higher, Microsoft Outlook Express 5.5 or higher, or Windows Mail
- One or more POP3 or MAPI email accounts

Also supports data migration from Windows 95, Windows 98, Windows Me, and Windows NT 4.0

[return to top](#) 

The registration screen asked me for my Mediacom email address, and I don't remember it. What should I do?

Your Mediacom email address can be found on the work order or documentation left with you at time of install. If you cannot locate that information please contact customer service [here](#). Please be sure to have your account number available to expedite your message.

[return to top](#) 

After I fill out the registration form what happens next?

You will receive a confirmation email that will include your license key. You can copy and paste key when prompted.

[return to top](#) 

What happens if I cancel my Mediacom account?

This software is being provided as part of your Mediacom Online service and would no longer be valid upon termination of your Mediacom account.

[return to top](#) 

What happens if I already have security software on my PC?

If you are running another Anti-Virus or Firewall product you will need to uninstall it, but don't worry, it's simple. Your Internet Security Suite download process includes how to uninstall other software depending upon the operating system you are running.

You do not need to uninstall anti-Spyware to install CA Anti-Spyware.

[return to top](#) 

How does a firewall work?

A firewall monitors all incoming Internet traffic and allows only what is known or trusted. The traffic enters through "ports" on your PC. There are over 65,000 ports available through Internet Protocol. Trying to manually restrict these would be impossible. Firewall software does this by opening ports that need to be open and closing off ports that do not. It also makes your computer invisible to the Internet making it harder for "Hackers" to gain access to your PC.

[return to top](#) 

I think I have a Virus on my PC.

If you have a reason to believe that you have a virus on your computer, please follow the steps outlined in this document:

1. Run the Microsoft Windows update to apply any critical patches necessary. Please [Click Here](#) to run the update utility.
2. Update the Anti-Virus signature files. Please [Click Here](#) for instructions.
3. Shut down all Network Drives to contain the virus and perform the following steps on each computer. In a home network where you are the administrator, you can easily unplug your network cable or Internet connection to contain the virus.
4. Disable the system restore feature. Please [Click Here](#) for instructions. (only for Windows XP and ME users)
5. Restart Windows in *SAFE MODE*. (If you are unsure of how to boot your computer in Safe Mode, [Click Here](#))
6. Go to Start > All Programs > CA > CA Internet Security Suite > CA Anti-virus and open the program.
7. Click on the "Overview" tab on the left-hand side.
8. Click on "Scan My Computer for Viruses" to start a system scan.

[return to top](#) 

Where is my License Key?

Locating Your License Key:

During the installation, you will be asked to insert your license key to unlock the product. The license key is a 20 character alpha-numeric code.

You can locate your license key within the welcome email that was sent to you by your Mediacom. If you did not receive the welcome email containing the license key, please contact us for further assistance.

Inputting Your License Key:

Here are some tips when entering in your license key:

- Make sure there are no extra spaces before or after the code.
- Try copying and pasting the license from your welcome email. Make sure you do not copy any extra spaces on the end of your license.
- Do not include the 10 digit customer number
- If the NEXT button (during install) is grayed out the problem is probably that you didn't finish entering the license.

- Please take special care when entering the numbers and letters. Some commonly confused characters are
 - 1 (number one), l (lower case L), and I (upper case i)
 - The number 0 (zero) and O (letter O).
 - The letter X (X), and the letter K (K).
 - The number 3 (three) and the letter J (J).
 - The number 4 (four) and the letter H (H).

[return to top](#) 

I have finished downloading, where do I find it?

The best way to know where your download saved, is to pay close attention to the "Save As" window at the beginning of the download process. Once you have clicked the download button and selected the option to save the file, you will be given the "Save As" window, which shows you exactly where your download is being saved to on your computer.

If you know the filename, you can do a search on your computer for it. Do not rename the file you're downloading, it may cause installation problems.

[return to top](#) 

CA Anti-Virus has detected a Trojan on my computer. What should I do?

A Trojan is a malicious program that masquerades as a legitimate program. It may look like it is a system file or a patch or even a game but when activated, it runs some other malicious activity.

CA Anti-Virus will automatically delete Trojans when they are detected if they are not "in use" by the system. If the file is "in use" by the system, please follow the steps below to remove it from your computer:

Attempt to delete the file manually:

1. Copy down the file name that was given during the virus scan. This will be in the last line of the scan results window.
2. Search for the file by going to START>Search for files/folders, entering in the file name.
3. Once the file is found, right-click on it and select delete or highlight the file and hit delete on your keyboard.
4. If this works, remember to delete the file from your recycle bin as well. If it doesn't work, move on to the next option.
5. Reboot the computer into Safe Mode and Delete the file:
 1. For instructions on how to boot into Safe Mode, [Click Here](#).
 2. Once you are in Safe Mode, search for the file by going to START>Search for files/folders, entering in the file name.
 3. Once the file is found, right-click on it and select delete or highlight the file and hit delete on your keyboard.
 4. If this works, remember to delete the file from your recycle bin as well. If it doesn't work
 5. Restart Computer

[return to top](#) 

What is the difference between the Anti-Spam Folder (visible in the list of Outlook mail folders) and the Anti-Spam Folder Quarantine Panel (accessible from the Quarantine option of the Anti-Spam Folder menu)?

The Anti-Spam Quarantine Panel displays only NEW, un-reviewed messages that have been quarantined; the Anti-Spam Folder contains un-reviewed messages, messages that have been blocked, and messages that were reviewed using the Quarantine Panel but which were not Approved. Generally, the Quarantine Panel provides the most convenient way to scan new quarantined messages. The Anti-Spam Folder is used when searching for a specific message that one suspects was quarantined.

[return to top](#) 

Does Anti-Spam automatically delete inbound messages that it considers to be junk email?

No. Anti-Spam gives you full control over all of your email. Depending on the email address of individuals who send you email, Anti-Spam delivers messages to one of two mail folders:

- Inbox: only email from Approved Senders is delivered to your Inbox
- Anti-Spam Folder: email from unknown senders is delivered to your Anti-Spam quarantine folder for later review

[return to top](#) 

Can I use Anti-Spam with my AOL mail?

Anti-Spam can be used with AOL mail if you install additional software (e.g. eMail2Pop) that can access AOL mail and make it available to Microsoft Outlook. For more information about AOL2POP and instructions for accessing AOL mail from Microsoft Outlook, please visit <http://www.email2pop.com>

[return to top](#) 

How does Anti-Spam interact with Outlook rules?

Both Outlook rules and Anti-Spam compete with Outlook to receive notifications of new messages. Unfortunately, Outlook doesn't guarantee a delivery order for these notifications, so sometimes Anti-Spam might get notified first and sometimes Outlook rules might be notified first. This means that sometimes an Outlook rule may move a message into another folder before Anti-Spam has a chance to look at it and determine whether or not it is spam.

A related issue you may run into is that new mail notification may not appear to work when you receive mail that Outlook rules filtered into another folder. The reason for this is that in order to prevent Outlook from notifying you of new mail when you receive spam, Anti-Spam takes over new mail notification. It only does this notification when there is new mail in your Inbox when it runs. So if your Outlook rules runs first and moves a message into another folder, Anti-Spam won't notice this new email and won't notify you. As a workaround, it's possible to edit some of your rules and set them to play a sound in addition to moving the message into a folder.

These are both known issues and we're looking into resolving them for a future release.

[return to top](#) 

How do I install the Firewall?

1. The install-shield will run. Read the information on the first screen then click on Next.
2. The next screen asks you to choose a Typical or Custom install. We recommend that most users choose the Typical Installation.
3. Click next and the set up will install the product.
4. After Installing, the product will ask you to review the default settings. Click next to proceed and review the settings.
5. Next it will ask you to set up the "Pre-configured Options"
6. Next it will ask you to set up your Network through the Network Configuration Wizard. You MUST allow the network through in order to be able to connect to the Internet.
7. You will be prompted to reboot your computer. This is necessary for the driver to take effect. You may restart your computer now or later to complete the installation process.

[return to top](#) 

What if I have more questions regarding this software?

Visit <http://home3.ca.com/Support/techsupport/issplus.aspx> for more information.

[return to top](#) 

What is a virus?

A computer virus is a form of malicious software – also referred to as “malware” (derived from the combination of the words malicious, and software).

The forms of malware that anti-virus products commonly protect against include:

- Viruses – a small program that attaches itself to another program or document, and replicates with the potential to cause damage.
- Worms – specifically engineered to make extensive use of email to spread them rapidly.
- Trojans – programs that pretend to be something harmless but have a damaging or otherwise malicious intent.
- Zombies – programs that install themselves on PCs, and remain dormant until an external event triggers them into action. These could do damage to your PC, steal your personal information and send it to an unauthorized email account, or even open up remote control access to your PC.

All of these forms of malware are commonly referred to simply as “viruses”.

[return to top](#) 

How do anti-virus products work?

Anti-virus products provide protection by detecting viruses, and then disabling or removing them from your PC. Detecting viruses is the job of the anti-virus “engine”, which scans your PC, looking for the tell-tale signatures of these malicious programs. Once detected, the software will take the appropriate action, such as clean, delete, or quarantine.

[return to top](#) 

How do viruses spread?

Viruses today are typically spread via email, but can also be spread by sharing disks, network drives, or Internet downloads. Viruses cannot spread on their own and must be run (or executed) by someone to cause damage. Boot sector viruses spread when a user inadvertently boots their PC from an infected disk. Macro viruses can spread by simply opening an infected document.

[return to top](#) 

What damage can viruses cause?

The type of damage viruses can do varies dramatically. Some of them do a great deal of damage to files, or even destroy the contents of a hard drive, while others install programs intended to corrupt or steal information from your PC.

[return to top](#) 

What makes CA Anti-Virus different from the rest?

CA serves major corporations, government entities, and educational institutions worldwide. CA Anti-Virus gives home users powerful technology used by these organizations, in a format that's both easy-to-use and affordable. The CA Security Advisor Team, a global network of threat research labs focused on PC protection, detect and design protection against virus threats 24/7.

[return to top](#) 

Why does anti-virus software need continually updated signature files?

Since new viruses are released on a daily basis, it is critical that the anti-virus software you use is updated with new virus signatures to provide protection against the most current threats. CA Anti-Virus provides daily, fully automatic updates to help defend against the latest threats.

[return to top](#) 

How does CA Anti-Virus provide automated updates?

CA Anti-Virus is configured to automatically check and update virus signatures via a standard Internet connection. This process is completely automated and does not require user intervention.

[return to top](#) 

How can CA Anti-Virus protect me from tomorrow's viruses today?

Heuristic scanning engines enable CA Anti-Virus to detect even unknown viruses by analyzing file characteristics to prevent potential infection. Once a specific virus is added to our detections, CA Anti-Virus will also detect other iterations or variations of that virus. This way, when a new virus is created that uses a similar "fingerprint" as the previous virus, CA Anti-Virus will automatically detect the new virus.

[return to top](#) 

Who tests and certifies anti-virus software?

There are several independent organizations that test and certify anti-virus software. CA Anti-Virus is tested and certified effective by ICSA Labs, Virus Bulletin and West Coast Labs.

[return to top](#) 

Anti-Spyware FAQ

What is spyware?

Spyware is the common term for a wide variety of non-viral programs that are typically installed onto a user's PC without their knowledge. Spyware can steal your personal information, switch your home page, re-direct your web searches, display annoying ads, slow your PC to a crawl, or even control it remotely. Spyware comes in many shapes and sizes; some are simply an annoyance, while others threaten security and privacy.

Common types of spyware include:

- Spyware – tracks information about you, your computer, and your surfing habits
- Adware – displays unwanted advertising that can slow your computer to a crawl
- Keyloggers – can record every keystroke you make, then steal your passwords and other personal data
- Browser Hijackers – can change your browser home page and search results
- Remote Access Trojans (RATS) – allows attackers to remotely control your computer

[return to top](#) 

How do I get infected with spyware?

Spyware can enter your PC through everyday web browsing, unauthorized software downloads, peer-to-peer file swapping, email attachments, instant messaging and chat sessions, bundles with legitimate software, hacker website downloads, and "drive-by" installs from websites.

[return to top](#) 

Why do I need anti-spyware software?

Spyware can lead to anything from PC crashes to increased spam to identity theft. These threats are rapidly proliferating and represent a major security and privacy risk. Anti-spyware software is designed to detect and remove these threats.

[return to top](#) 

If I already have anti-virus software, do I need anti-spyware software?

Your anti-virus protection is important - it detects and removes viral threats. But your PC can be infected with other dangers such as spyware. Anti-spyware software is designed to stop these threats, which have unique properties that can remain hidden on your PC and cause havoc. CA Anti-Spyware detects and removes a wide range of spyware threats, making it a powerful complement to your anti-virus defense.

[return to top](#) 

Why not use free anti-spyware software?

Free anti-spyware products typically do not offer all of the features and functions available in CA Anti-Spyware - such as real-time protection, a spyware information database, logging, support and automatic updates. Also, free products typically cannot afford to invest heavily in research and development, meaning their products may not be as effective in detecting and removing a wide range of threats. In addition, free anti-spyware products usually do not offer the same level of customer service and technical support.

[return to top](#) 

Personal Firewall FAQ

What is a firewall?

A firewall is an important first line of defense for computer security. A firewall is software or hardware that acts as a barrier between your PC and the Internet. It prevents unauthorized programs or users from accessing your PC, and hides your Internet-connected PC from view. All information leaving and entering your PC must pass through the firewall. It ultimately helps keep hackers away from your personal and confidential data.

[return to top](#) 

Why do I need a firewall?

In today's world of computing, several layers of protection are needed in order to defend your confidential data from hackers. Every PC connected to the Internet is a potential target. Computers are under constant attack from cyber vandals. Whether your connection is dial-up, DSL, or always-on, a firewall is necessary to stop intruders from getting into your PC.

[return to top](#) 

What kinds of threats do firewalls protect against?

Firewalls help protect against hackers and online intruders who steal personal and confidential data that could lead to identity theft. Firewalls inspect each "packet" of data as it arrives on either side of the firewall – inbound from the Internet, or outbound from your computer. The firewall determines whether it should be allowed to pass, or if it should be blocked.

[return to top](#) 

If I already have anti-virus and anti-spyware software, do I need a firewall?

Yes. CA Personal Firewall stops unauthorized access and hides your PC from possible hacker attacks. Firewalls protect you from things that anti-virus software and anti-spyware software are not designed to find.

Anti-virus software detects and removes viruses, while anti-spyware software detects and removes spyware, adware, and other non-viral malicious code. Accordingly, CA Personal Firewall is the perfect complement to anti-virus and anti-spyware software, providing a key component of a multilayered security strategy.

[return to top](#) 

Anti-Spam FAQ

What is spam?

Spam is the common term for electronic 'junk mail' or unwanted messages sent to a person's email account.

[return to top](#) 

Why is spam a problem; can't I just delete spam from my Inbox by hitting Delete?

Today, a large percentage of all email is unsolicited, unwanted spam. The billions of spam messages circulating across the Internet can disrupt email delivery, degrade system performance, and reduce overall productivity. Deleting spam emails seems like the simple solution, but if you add up the time spent deleting every spam email you receive, you lose a significant amount of productivity.

[return to top](#) 

What kinds of threats does an anti-spam product protect against?

Spam messages can contain offensive material, can be used in fraudulent phishing attacks designed to steal your personal information, and can even be used to spread viruses. Spammers can also take control of your computer in order to send spam to others, from your PC. These compromised home computers - collectively referred to as 'botnets' - can be used to send bulk emails by the millions.

Therefore, spam is not only a nuisance that affects your productivity - it can also be a serious threat to your security, privacy, and the health of your PC.

[return to top](#) 

How do I get spam?

Spammers often use bulk email programs to send out their unsolicited messages to lists of email addresses that are often collected without the recipient's knowledge. There are several ways spammers obtain these email addresses:

- Harvesting from Websites – Most companies list email addresses and contact information on their websites. Spammers use web-crawlers to search for and collect these email addresses.
- Mailing Lists – Many people sign up for mailing lists for newsletters, news alerts, coupons, special offers, and other interests. Spammers can often purchase or even steal these mailing lists.
- Usenet Posting – Spammers can also use bots to cruise newsgroups on Usenet in order to collect email addresses.
- Coincidental – Your email address may be unique to your Internet Service Provider (ISP), but it may also be used by several other people using different ISPs. Spammers use the front part of email addresses and change the ISP name to create a list of several email addresses that might be valid.
- Dictionary Attacks – Spammers make educated guesses on email addresses by stringing together common names and words.

[return to top](#) 

Can't I get rid of spam emails by unsubscribing?

Not always. Any response to spam emails confirms the accuracy of your email address, and may result in even more spam messages.

[return to top](#) 

How can I solve my spam problem?

CA Anti-Spam is the easy-to-use, effective anti-spam solution that blocks unwanted spam. CA Anti-Spam allows you to see important messages from people you know while blocking questionable messages from people you don't.

[return to top](#) 

Website Inspector (Anti-Phishing) FAQ

What is phishing?

Phishing generally refers to email messages that appear to come from trusted companies, but then attempt to direct you to a fake website, where you are asked to provide sensitive personal information (passwords, account numbers, credit card numbers, and so on). This information can then be used by the creators of the website to commit identity fraud. Phishing emails are designed to appear legitimate, and the websites often look identical to the legitimate company's website. Phishing attacks are not limited to email, however; they can also occur through instant messaging, in web pop-ups, or through spyware programs that may have been secretly installed on your PC.

[return to top](#) 

What is the risk in doing business on the Internet?

The Internet has become a popular media for e-commerce and online banking. As the business grows, scammers find ways to fool unwary users into submitting personal and confidential details to fraudulent sites, who can misuse that information. Other sites hide their identity and tempt users to pay for goods and services they will never receive.

What are the most common methods of Internet fraud?

The main Internet fraud methods are:

- Pharming - A set of technical tricks that actually changes the destination of the URL that you see in your browser, and directs you to an "undercover" site. In other words, if you type www.mybank.com, you may think you are accessing your bank, but you're actually entering a scam site.
- Sites "without identity" or with hidden identity - Sites that deliberately hide their ownership, making it harder to find the owner after a fraud has been committed at the site.
- Sites that collect personal or confidential information and do not keep the details secure - Sites that share your private information and email address with other sites for a profit.
- Spyware, Trojans & Keyloggers – Sites that secretly install malicious software on your PC, to track your use of the computer and send the information to those who intend to misuse it.

[return to top](#) 

What is CA Website Inspector?

CA Website Inspector helps protect you from phishing attacks, Internet fraud attempts, and malicious websites. It provides a browser toolbar that allows you to verify the identity of the website you are visiting, and offers an easy-to-understand risk assessment informing you whether it's safe to visit the site, or send personal information to the site. CA Website Inspector also checks any links received in email, instant messenger and office applications, and verifies whether the site is safe.

[return to top](#) 

What is the CA Toolbar?

After installing CA Website Inspector, you'll notice an additional toolbar in your browser window. It shows you the physical address of the real owner of the site you're viewing. It also evaluates every site you visit and warns you when you access dangerous or fraudulent sites. The CA Toolbar helps keep you safe and informed while browsing, allowing you make educated decisions about trusting the sites you visit.

[return to top](#) 

What browsers does the CA Toolbar support?

The CA Toolbar currently supports Internet Explorer 5.0+ and Firefox 1.0+.

[return to top](#) 

What is the CA Link Advisor?

The CA Link Advisor is another component of CA Website Inspector designed to keep you safe and informed while using the Internet. It works within your email, instant messenger, and office applications to show you vital information about the sites behind the links you intend to visit, before you even click on the link. It evaluates every link and provides you with the following information:

- Which site will you really visit
- Which company stands behind the site
- Is it safe to deal with the site
- Are there any known risks visiting the site

[return to top](#) 

What applications does Link Advisor support?

CA Link Advisor works with a variety of applications including Microsoft Word, Outlook and Outlook Express, Windows Mail, Yahoo! Instant Messenger, ICQ, Google Talk, and more.

[return to top](#) 

Why do I need parental controls software?

Despite its benefits, the Internet has also become a medium to communicate things that many households would consider dangerous, offensive, sexist, racist, or otherwise inappropriate for their family. Parental controls software is one way for parents to take the initiative to create an Internet environment that they consider safe.

[return to top](#)

What are the most common risks to children on the Internet?

Studies have shown that children can be inadvertently exposed to pornography or other inappropriate content, or can intentionally view it; can be solicited for sex while online; or can simply use the Internet in ways that a parent would consider inappropriate or excessive.

[return to top](#)

How do parental controls products work?

Parental controls software allows a parent to control and/or monitor the online activities of their child or children. Parental controls products allow parents to block offensive websites, set time limits on Internet usage, and view reports that summarize the online activities of the child.

[return to top](#)

Desktop DNA® Migrator (Data Backup and Transfer) FAQ

What is CA Desktop DNA Migrator?

CA Desktop DNA Migrator helps you backup and restore your PC's "DNA" – everything about your PC that is unique to you. It also allows you to easily transfer (migrate) that DNA from one computer to the next. With just a few clicks, you can preserve user settings, address books, data files, favorites, printer settings and numerous other unique settings and preferences that you don't want to lose. With its user friendly wizard interface, CA Desktop DNA Migrator offers unprecedented control and flexibility.

[return to top](#)

What is a PC's DNA?

Each person modifies their PC to fit their needs, jobs and preferences, making their PC unique. Just like humans, computers are all unique as defined by their DNA. A computer's DNA consists of system and application settings, preferences and data files and folders – everything that makes your PC unique to you - including:

- All of your Contacts and Address Books
- Your Email, Accounts, Calendars and Settings
- All of your Documents, Pictures and Music
- Favorites, Bookmarks and all Internet Connection Settings
- Printer, Network and Wireless Settings
- Microsoft Office Settings and Templates
- Favorite Background and Display Settings
- Shortcuts and Task Manager Settings
- Settings for hundreds of the most popular applications

[return to top](#)

Why do I need a data backup solution?

In the event of an unforeseen incident – for example, a virus or system crash – it's important to keep a "copy" of your PC's DNA, and have the ability to restore your PC to its original state before the incident occurred. CA Desktop DNA Migrator allows you to easily backup, protect and restore your PC's DNA after a disaster event.

[return to top](#)

Why do I need a data migration solution?

Getting a new PC is great. What's not so great is trying to move your PC's DNA from your old computer to your new one. Without your old PC's DNA, you will spend hours, maybe days, relearning the way your new PC works. CA Desktop DNA Migrator is the quickest and easiest way to safeguard and transfer your PC's DNA to your new or upgraded PC. By transferring your DNA from your old PC to your new PC you will be up and running quickly, taking advantage of your new PC's features and functions while still enjoying the familiar desktop environment settings, data and connections of your old PC.

[return to top](#) 

What is the difference between a Typical and Custom Migration?

A Typical Migration takes the guesswork out of migrations by predefining the most common system and application settings, files and folders. With a few clicks you can perform a complete migration that automatically transfers:

- Desktop, dial-up, networking, and system settings
- Application settings*
- My Documents folder and all sub-folders
- Document types*

A Custom Migration takes power, control and flexibility even further by giving you the option to customize settings for special migration needs:

- Select a Real-Time or Deferred migration
- Include or exclude certain settings for:
 - Desktop – Shortcuts, taskbar, wallpaper, display, etc.
 - Network – Dial-up, TCP/IP, etc.
 - Printers
- Include or exclude supported application settings
- Include or exclude files and folders
- View files and folders in a simple checkbox tree - checked items will be included in a migration, unchecked items will not be included
- Create rules to include certain file types or specific folders or files from all local drives

* CA Desktop DNA Migrator supports the most popular business, graphic and multimedia applications, such as Microsoft Excel, Outlook, Outlook Express, PowerPoint, and Word; Lotus Notes; as well as the complete line of Adobe graphic and Macromedia products.

[return to top](#) 

What is the difference between a Deferred and a Real-Time migration?

A Real-Time migration quickly streams your DNA information directly from a source system to a destination system. Performing a Real-Time migration requires that the two computers you wish to migrate be connected to each other by a local area network (LAN) or an Ethernet crossover cable. A Deferred migration creates a self-extracting DNA file directly to your desktop or removable media. It then allows you to apply the DNA file to the destination system or keep it for system back-up or future migration.

[return to top](#) 

Can CA Desktop DNA Migrator move a PC's DNA between different versions of applications and Windows operating systems?

Yes. For example, CA Desktop DNA Migrator will move Office 97 settings on a Windows 95 machine to Office XP on a machine running Windows XP.

[return to top](#) 

Does CA Desktop DNA Migrator migrate Outlook settings and associated mail files?

Yes. CA Desktop DNA Migrator will not only migrate settings and associated mail, but can also apply them to the destination's default configuration; in other words, from the Outlook file in the older versions to the new default location.

© 2007 CA, Inc. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

© 2007 Mediacom Communications Corporation. All Rights Reserved. Mediacom Online, OnMedia and Mediacom Power Pak are service marks, and Mediacom; Mediacom Digital, and Mediacom OnDemand are the registered service marks of Mediacom Communications Corporation.