



January 28, 2003

[Log On](#)

**NEWSLETTER**

[Newsletter Archive](#)

**CONTENTS**

[News](#)

[Security Discoveries](#)

[Topics](#)

[Departments](#)

[Authors](#)

[Code Library](#)

[Books & Reviews](#)

[Product Reviews](#)

**Q & A**

[Forums](#)

[FAQs](#)

**SUBSCRIBE/RENEW**

[Print Newsletter](#)

**Security Administrator**

**FREE E-Newsletters**

Please subscribe me to:

Security UPDATE & Alerts  
[Details](#) | [Archive](#)

**Discussion Lists**

Win2K Security List  
[Details](#) | [Archive](#)

Security How-To List  
[Details](#) | [Archive](#)

Email:

[More Email Newsletters](#)



**NETWORK TOPICS**

- [Windows & .NET Magazine](#)
- [CertTutor.net](#)
- [Connected Home Magazine](#)
- [Exchange & Outlook Admin](#)
- [Mobile & Wireless Solutions](#)
- [Security Admin](#)
- [Storage Admin](#)

**VIP SUPER CD/VIP MEMBERSHIP** [Log On](#) [Learn More](#)

ate and federal century, the 1972...  
 e the first of its bers are asking ers to give mon-  
 Monterey Trail- site that dates  
**Get it all on the SuperSite for Windows!**  
**CLICK HERE!**  
 Then the 40-year-old Agnew en- The deeper tale behind

- [SQL Server Magazine](#)
- [Windows Scripting Solutions](#)
- [Windows Web Solutions](#)

## NETWORK RESOURCES

- [WinInfo News](#)
- [SuperSite for Windows](#)
- [Forums](#)
- [Windows NT/2000 FAQ](#)
- [JSI FAQ](#)
- [IT Buyer's Network](#)
- [Windows IT Library](#)
- [Subscribe/Renew](#)
- [Events](#)
- [Mobile Edition](#)
- [User Groups](#)
- [Web Seminars](#)
- [White Paper Central](#)

Search



Advanced Help

InstantDoc



Site Sponsored by



Live NetIQ Security Webcast on 2/18. [Register now](#) for "Chaos to Control" featuring Kevin Mitnick.

January 17, 2002 | [Paul Thurrott](#) | [WinInfo](#) | InstantDoc #23801

## Complete text of the Bill Gates "Trustworthy Computing" Memo



**It's  
FREE!**



I'm still corroborating that this is the complete text, but my understanding that this is the [email](#) message Bill Gates sent to Microsoft's employees Wednesday. --Paul

-----Original Message-----

From: Bill Gates  
 Sent: Tuesday, January 15, 2002 5:22 PM  
 To: Microsoft and Subsidiaries: All FTE  
 Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our [.NET](#) strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring [.NET](#) is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing -- or able -- to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

When we started work on Microsoft [.NET](#) more than two years ago, we set a new direction for the company -- and articulated a new way to think about our software. Rather than developing standalone applications and Web sites, today we're moving towards smart clients with rich user interfaces interacting with Web services. We're driving the XML Web services standards so that systems from all vendors can share information, while working to make Windows the best client and server for this new era.

There is a lot of excitement about what this architecture makes possible. It allows the dreams about e-business that have been hyped over the last few years to become a reality. It enables people to collaborate in new ways, including how they read, communicate, share annotations, analyze information and meet.

However, even more important than any of these new capabilities is the fact that it is designed from the ground up to deliver Trustworthy Computing. What I mean by this is that customers will always be able to rely on these systems to be available and to secure their information. Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services and telephony.

Today, in the developed world, we do not worry about electricity and water services being available. With telephony, we rely both on its availability and its [security](#) for conducting highly confidential business transactions without worrying that information about who we call or what we [say](#) will be compromised. Computing falls well short of this, ranging from the individual user who isn't willing to add a new application because it might destabilize their system, to a corporation that moves slowly to embrace e-business because today's platforms don't make the grade.

The events of last year -- from September's terrorist attacks to a number of malicious and highly publicized computer viruses -- reminded every one of us how important it is to ensure the integrity and security of our critical infrastructure, whether it's the airlines or computer systems. Computing is already an important part of many people's lives. Within ten years, it will be an integral and indispensable part of almost everything we do. Microsoft and the computer industry will only succeed in that world if CIOs, consumers and everyone else sees that Microsoft has created a platform for Trustworthy Computing.

Every week there are reports of newly discovered security problems in all kinds of software, from individual applications and services to Windows, Linux, Unix and other platforms. We have done a great job of having teams work around the clock to deliver security fixes for any problems that arise. Our responsiveness has been unmatched -- but as an industry leader we can and must do better. Our new design approaches need to dramatically reduce the number of such issues that come up in the software that Microsoft, its partners and its customers create. We need to make it automatic for customers to get the benefits of these fixes. Eventually, our software should be so fundamentally secure that customers never even worry about it.

No Trustworthy Computing platform exists today. It is only in the context of the basic redesign we have done around [.NET](#) that we can achieve this. The key design decisions we made around [.NET](#) include the advances we need to deliver on this vision. [Visual Studio](#) [.NET](#) is the first multi-language tool that is optimized for the creation of secure code, so it is a key foundation element.

I've spent the past few months working with Craig Mundie's group and others across the company to define what achieving Trustworthy Computing will entail, and to focus our efforts on building trust into every one of our products and services. Key aspects include:

**Availability:** Our products should always be available when our customers need them. System outages should become a thing of the past because of a software architecture that supports redundancy and automatic recovery. Self-management should allow for service resumption without user intervention in almost every case.

**Security:** The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

**Privacy:** Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.

Trustworthiness is a much broader concept than security, and winning our customers' trust involves more than just fixing bugs and achieving "five-nines" availability. It's a fundamental challenge that spans the entire computing ecosystem, from individual chips all the way to global Internet services. It's about smart software, services and industry-wide cooperation.

There are many changes Microsoft needs to make as a company to ensure and keep our customers' trust at every level - from the way we develop software, to our support efforts, to our operational and business practices. As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable. Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers' view of us as a company.

In recent months, we've stepped up programs and services that help us create better software and increase security for our customers. Last fall, we launched the Strategic Technology Protection Program, making software like IIS and Windows .NET Server secure by default, and educating our customers on how to get -- and stay -- secure. The error-reporting features built into Office XP and Windows XP are giving us a clear view of how to raise the level of reliability. The Office team is focused on training and processes that will anticipate and prevent security problems. In December, the Visual Studio .NET team conducted a comprehensive review of every aspect of their product for potential security issues. We will be conducting similarly intensive reviews in the Windows division and throughout the company in the coming months.

At the same time, we're in the process of training all our developers in the latest secure coding techniques. We've also published books like "Writing Secure Code," by Michael Howard and David LeBlanc, which gives all developers the tools they need to build secure software from the ground up. In addition, we must have even more highly trained sales, service and support people, along with offerings such as security assessments and broad security solutions. I encourage everyone at Microsoft to look at what we've done so far and think about how they can contribute.

But we need to go much further.

In the past, we've made our software and services more compelling for users by adding new features and functionality, and by making our platform richly extensible. We've done a terrific job at that, but all those great features won't matter unless customers trust our software. So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve. A good example of this is the changes we made in Outlook to avoid email borne viruses. If we discover a risk that a feature could compromise someone's privacy, that problem gets solved first. If there is any way we can better protect important data and minimize downtime, we should focus on this. These principles should apply at every stage of the development cycle of every kind of software we create, from operating systems and desktop applications to global Web services.

Going forward, we must develop technologies and policies that help businesses better manage ever larger networks of PCs, servers and other intelligent devices, knowing that their critical business systems are safe from harm. Systems will have to become self-managing and inherently resilient. We need to prepare now for the kind of software that will make this happen, and we must be the kind of company that people can rely on to deliver it.

This priority touches on all the software work we do. By delivering on Trustworthy Computing, customers will get dramatically more value out of our advances than they have in the past. The challenge here is one that Microsoft is uniquely suited to solve.

Bill

[Click Here to buy a Reprint or Eprint of a Security Administrator Article](#)

## Topics

- [Security](#)
- [News and Analysis](#)

## Related Articles

-  [Find Related Articles](#)
-  [Related Products](#)

## Article Information

-  [Email this Article](#)
-  [Printer-Friendly](#)

## Reader Comments

 [Post a Comment](#)

[Johan Baneman](#) - It's a joke! Bill wrote "Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate..."

[More Comments >>](#)

### SPONSORED LINKS

- [FREE! Exchange 2000 eBook. New Chapters Available. Register Now!](#)
- [FREE performance boost. Find out what you're MISSING.](#)
- [FREE FAX SERVER TRIAL - Reduce FAX Charges 20-80%](#)
- [CommVault Galaxy-Backup/Restore in MSA for Enterprise Data Center](#)
- [Get the most from your Windows®-based Management Solutions!](#)
- [Limited Time Offer: Save on Microsoft licensing until 01/31/03](#)
- [FREE live trial-Award winning Backup & Disaster Recovery software](#)

### FEATURED LINKS

- [Join Paul Thurrott at the Microsoft Mobility Tour -- FREE!](#)
- [Windows & .NET Magazine - get a free sample issue!](#)
- [Save time and money - get our certification eBook!](#)



[Network Home](#) | [Network Map](#) | [Our Pubs](#) | [Our Events](#) | [Contact Us](#) | [About Us](#) | [Advertising](#) | [Affiliates/Licensing](#)  
Copyright © 2003 Penton Media, Inc., All rights reserved. [Legal](#) | [Privacy](#)