Microsoft

Security and Privacy

for Microsoft® Office 2010 Users

Mitch Tulloch

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2012932376
ISBN: 978-0-7356-6883-6

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Acquisitions Editor: Rosemary Caperton
Editorial Production: Diane Kohnen, S4Carlisle Publishing Services
Copyeditor: Susan McClung
Indexer: Maureen Johnson

Contents at a Glance

CONTENTS

Acknowledgments

I would especially like to thank the following individuals at Microsoft who peer-reviewed this book to ensure technical accuracy:

Nam Ngo, SDET II for PARC (Publishing, Authoring, Reading, and Collaborating)

Harold Kless, Senior Support Escalation Engineer for CSS (Customer Support Services)

Eran Kolber, Regional Director and Platform Value Evangelist

Didier Vandenbroeck, Principal Lead Security Program Manager for Office TWC Security, Microsoft Corporation

—Mitch Tulloch

Introduction

SECURITY AND PRIVACY issues with computers and computer networks are constantly in the news these days, and everyone seems to be concerned about them to some degree. Businesses everywhere are worried about having sensitive customer information such as credit card numbers or email addresses stolen, so they tell their information technology (IT) staff to make sure that everything is secure and locked down. And managers tell their office workers to follow corporate security policies and procedures closely or risk facing disciplinary consequences. As a result, the busy office workers sometimes feel as though they are between a rock and a hard place—management threatens them with the rock if they don't follow the security guidelines, and IT just seems to make it harder for them to do their jobs.

Compounding these pressures are the software applications that office workers use to perform their work. While productivity software like Microsoft Office can be rich in features and capabilities, businesses often commit too little time and money to train their workers adequately in effectively using such software. The result is that the busy office worker can become the weak link in an organization's efforts to secure and protect its information systems and data.

This book tries to fill the gap where Office is concerned, and it is intended as a guide to how to use the powerful security and privacy features of this platform effectively. Although the entire book applies to Office 2010, some of the content also can be helpful to businesses that use the cloud-based version of Office called Office 365.

Who This Book Is For

The target audience for this book is the Information Worker (IW), someone who works within an organization and whose primary job responsibility involves sharing, communicating, processing, or acting upon information stored on computer systems and networks. Workers in organizations of all sizes, from small businesses to large enterprises, will benefit from this book.

Assumptions

The primary prerequisite for readers of this book is that they should have basic to intermediate-level familiarity with the following Office applications:

- Microsoft Word 2010
- Microsoft Excel 2010
- Microsoft PowerPoint 2010

In addition, some familiarity with using Office 365 can be helpful but is not required.

How This Book Is Organized

Chapter 1, "Why Should I Care?" begins by addressing some general questions that the typical office worker should consider, such as:

- Why should I care about information security and privacy?
- Isn't that really the responsibility of other parties like management and IT?
- What's my own role in making sure our business information is kept secure and private?

After this come three chapters that involve different scenarios where fictitious office workers are faced with needing to understand and use the security and privacy features of Office to accomplish tasks for their jobs. These three chapters are titled:

- Chapter 2, "Alice Downloads a Document"
- Chapter 3, "Bob Prepares a Policy"
- Chapter 4, "Carol Collaborates on Some Content"

The appendix, "Where to Learn More," provides links to where the interested reader can learn more about the security and privacy features of Office.

You can read the book from cover to cover or simply jump to the chapter that interests you. But make sure you read Chapter 1 first, because it may help you start thinking about the subject in ways you haven't thought of before.

How to Get Support and Provide Feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata and Book Support

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site at oreilly.com:

http://go.microsoft.com/FWLink/?Linkid=242816

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

At Microsoft Press, your satisfaction is our top priority and your feedback our most valuable asset. Please tell us what you think of this book at

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in Touch

Let's keep the conversation going! We're on Twitter:

http://twitter.com/MicrosoftPress.

CHAPTER 1

Why Should I Care?

IN THIS CHAPTER, YOU WILL

- Learn why it's important for office workers to consider security and privacy as they perform their jobs.
- Learn about the responsibilities of management and IT in safeguarding the information systems and sensitive business data of an organization.
- Learn that office workers share joint responsibility for the security and privacy of business information with management and IT.
- Learn how what the office worker chooses to do can have either a positive or negative impact on the security and privacy of an organization's network, systems, and data.

SO YOU WORK in an office and you use Microsoft Office programs like Microsoft Word, Excel, and PowerPoint to do your job. Your boss has told you to be careful about security because of the recent virus infection the company experienced. And he's told you to be careful when publishing documents online and make sure you remove anything private from the document like comments, tags, and the name of your manager. He's also reminded you to adhere carefully to the standards and guidelines published in the company's Security and Privacy Policy document available on the corporate intranet.

What's the big deal? Isn't security the responsibility of the guys in the IT department down on the third floor? Shouldn't the firewall block viruses from our network? If it doesn't, those IT guys should be fired—it's not my fault if a Word document I open has a virus in it.

And who reads those policy documents anyway? They're so long and wordy and hard to follow. I'm sure nobody will be harmed if I accidentally leave some hidden comments in a document I publish on our company's website. Besides, how do you even know that hidden stuff is there?

I just need to do my job and wish IT would do theirs, and those guys in management should just stay out of my way . . .

Hey, It's Not *My* Responsibility!

Does the above thinking sound familiar? If you work in an office and use Office software, then you've probably thought (and possibly expressed) those kinds of ideas from time to time. But is such a position really justified? Is security only the responsibility of the IT department? And is protecting the privacy of confidential business information only the responsibility of upper management?

To a certain extent, your thinking is correct. Ensuring the security of an organization's network, computers, and other connected devices such as smartphones is, in fact, one of the key roles of IT. The IT department also is primarily responsible for ensuring that files and other data stored on the network and accessible to you via your computer or smartphone are safe to work with and protected against unauthorized access. So you should be able to open and work with documents, spreadsheets, and other files without worrying whether they contain viruses or other malware. You should be able to just do your job, provided that IT is doing its job properly, right?

But what if you think the controls that IT has put in place on your network are too restrictive? What if you want to circumvent these controls so you can "just do your job"? For example, suppose that your IT department has locked down Office so that macros can't run in documents. You think, however, that macros can be useful to "help you do your job better under certain circumstances," so you try to work around the controls IT has put in place by bringing your own personal laptop to work and copying certain company documents to your laptop so you can add macros to them. Then, when you're finished working on these documents, you copy them back to your office computer so that they can be saved to the network share where they are stored.

You've just broken the security and privacy model of your organization in two ways. First, you've found a way to bypass physically the security and privacy controls that IT has put in place on your company's network. This means you've technically compromised your organization's security. And second, you've deliberately chosen to ignore the rules your company has put in place to safeguard its business operations and data. What I mean is, the written security policy document published on your corporate intranet probably contains a statement that reads something like this:

> ***"Office staff are strictly prohibited from attempting to circumvent any of the security or privacy controls that IT has put in place on the company network and its resources."***

In other words, not only have you compromised your company's security, but you've also violated their security policies. If you get caught doing this, you may well face consequences!

So saying that security and privacy are solely the responsibility of IT and management and that as an office worker, you have absolutely no responsibility in these matters is simply not true. What is true is that the parties *primarily* responsible for ensuring the security and privacy of business computing resources and data are (a) upper management, which defines and publicizes the policies that all users (including IT) should follow, and (b) the IT department, which implements controls that enforce those security/privacy policies that can be enforced solely by technical means.

Here's an analogy that might make this clearer. Saying that network and data security is solely the responsibility of your IT department is like saying that the maintenance of your car is solely the responsibility of your mechanic. But if you're driving along the highway and your oil light is flashing and you ignore it, you're going to have a problem—and it's clearly not your mechanic's fault (unless he forgot to put in the oil when you last had your car serviced).

Likewise, saying that confidentiality of business information is solely the responsibility of management is like saying that you can safely ignore the road signs and traffic lights when you drive your car. If you have an accident as a result of doing something like that, good luck trying to blame anyone other than yourself!

So yes, you, the lowly office worker, should—and must—care about the security and privacy of your company's information system and resources. You do have a role in protecting your company against the theft, destruction, corruption, or accidental loss of sensitive business files and data.

TECHNICAL LIMITS TO SECURITY/PRIVACY ENFORCEMENT

Some security and privacy policies can't be enforced solely by technical means, or at least, it can be very difficult or expensive and often extremely intrusive to those involved if you try to enforce such policies by technical means. For example, let's say your organization has a policy that says, "Staff shall not make copies of company documents and take them off company premises." For IT to enforce such a policy through technical means alone, they could try disabling the Clipboard and all USB drive functionality on users' PCs so they can't copy and paste text from sensitive business documents into Notepad and save the text file onto a USB flash drive. Doing this, however, clearly would make it difficult for users to perform many work-related tasks.

A better alternative might be to implement a *Digital Rights Management System (DRMS)* on the company's network so that users can view and work with documents but not copy their content or open them on non-corporate devices.But this technical solution to enforcing the company's "shall not make copies" policy has two potential problems associated with it. First, it costs money to do this—the business may need to buy an additional server, pay licensing fees to the DRMS vendor, and create a training program to educate users on how to work with DRMS-protected documents. Of course, if management believes that the added security and privacy DRMS can provide the company is worth the money it takes to procure, implement, and maintain the system, then this problem can be overcome. And if you are a user in an organization that has a DRMS in place, you'll have to learn to adjust to how this affects the way you work.

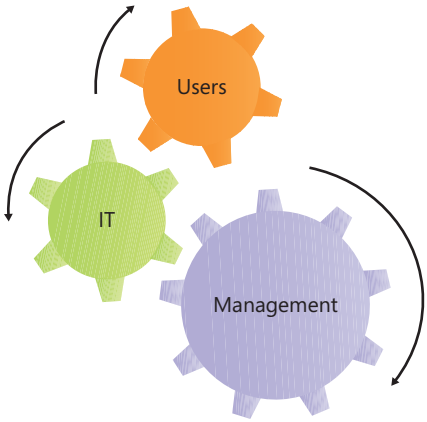
The second problem, however, is trickier: No security is bulletproof, and even DRMS can be circumvented. For example, all it takes is a camera-equipped cellphone for the user to take a photo of a DRMS-protected document displayed on her computer screen, and then she can walk out of the building with sensitive business records in her pocket. Or a user could simply take a photo of his computer screen and then email the photo using his cell phone. To prevent such things from occurring, the organization would need to confiscate all users' cell phones when they enter the building, store them somewhere, and return them to the users when they leave. This, of course, probably will be seen as a huge inconvenience by some users, and some of these people may try to smuggle their cell phones past the security personnel. The organization then may try to create a technical solution to this new problem by installing a walk-through metal detector at the entrance to the building, but such a solution is not only costly, but is also extremely intrusive to users who may face body searches when something they're carrying (which may be perfectly innocent) sets off the detector.

The bottom line here is that many, if not most, security/privacy breaches can't be prevented by technical means alone. Organizations also need easy-to-understand and well-communicated security policies and be consistent in how they enforce them. That's because users indeed are often the weak link in ensuring the security and privacy of an organization's confidential business information.

What's My Role in This?

Individuals who work in an office as you do probably tend to think that your work situation can be summed up with something like this:

What you should keep in mind, however, is the close interconnectedness in the way that a company actually works. As the illustration here suggests, the security and privacy of an organization's computer systems and the information they store and manage are the responsibility of everyone involved: the management team, the IT department, and you, the user:



Regardless of how you may think from time to time when the going gets tough at the office, the fact is that you're an essential cog in the gear chain that drives your organization's business forward and keeps its profitability on track. And this is especially true in the areas of information security and privacy, where your actions may contribute either positively or negatively in leading the business towards success or failure.

Let's consider the positive first. How can you, a lowly office worker, contribute to ensuring that your company's business systems and data are secure and kept confidential?

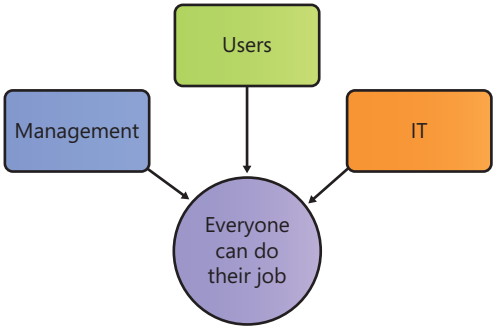
- Do your best to not just comply with company security policies, but also understand why they are important. Remember, if the business fails, you'll lose your job, too.
- Understand that not every frustrating, annoying, or even maddening policy that upper management decrees originated from them. Organizations today are often legally required to comply with a host of rules and regulations laid down by various levels of government. So sometimes their hands are tied when it comes to certain privacy and security policies they must institute in the organization.
- Do your best to be friendly and polite in all your dealings with IT, especially with help-desk incidents. Technology is constantly changing at a rapid pace, and few can keep on top of all the changes. This can make IT a maddeningly challenging field to be in, so you need to understand the pressures that IT staff face each day. Also, remember that those help-desk people are trying to do their jobs, just as you are.
- Do not try to circumvent the security controls that IT has put in place on your company's network. Those controls are there for a reason—usually to protect the organization's systems and data, but sometimes simply to make life easier for IT staff.
- Seek out and use the appropriate communications channels for providing feedback to management on company security policies and for making requests to IT for new hardware, software or services. Be sure to make the business justification clear for any changes you request from IT. If they indicate that they can't do as you request, there's probably a good reason for this.

Finally, what about the negative side of all this? What could you, the exasperated office worker, do that might contribute negatively to the security of your company's business systems and privacy of their sensitive business data? Here are a few things you should avoid doing if at all possible:

- Do not deliberately do anything that's expressly forbidden by the corporate security policy. This might include things like taking work home by copying files to unencrypted USB flash drives, telling others your password so they can check your email for you when you're sick at home, using your personal cell phone for making confidential business calls, clicking links in phishing emails instead of immediately deleting the emails or reporting them to the help desk, and so on.

- Do not deliberately try to do something that is normally prevented by the controls that IT has put in place on your network. Examples might include trying to disable the antivirus software on your computer because it makes the computer run slowly, saving business documents directly on your desktop when you are fully aware that IT backs up only your Documents folder and not the files on your desktop, tampering with your company-issued smartphone so you can install Angry Birds on it, and so on.
- Do not fail to communicate clearly, directly, and politely with IT or management when you believe that a certain IT control or certain company policy is preventing you from doing your job efficiently. Any company that values the future of its business must have effective lines of communication in place for users to communicate their needs, problems, and frustrations concerning their ability to do their job because if the user cannot do his or her job, the company's bottom line will be affected.

Think of it this way: In a healthy organization, each entity must try to make every other entity's task easier and safer to perform, as shown here:



But what if your organization isn't like this? What if it's horrible to work there, and the place is full of seemingly pointy-headed managers and cynical, know-it-all IT personnel? What can you do then?

Well, remember that if all else fails, you can always vote with your feet. Why Dilbert has kept putting up with his pointy-haired manager over the years is something that's quite beyond me. If he were half the smart guy that he seems to be in the cartoon (see *http://www.dilbert.com*), Dilbert would quit his job and find a better company to work at, or even start his own business!

Summary

Security and privacy should be the concern of everyone in an organization, not just IT or management.

The role of IT in an organization's security and privacy is to design and implement technical controls that help safeguard the organization's network, systems, and data.

The role of management in an organization's security and privacy is to publish and clearly communicate the written security policies that explain what users should and should not do to help safeguard the organization's network, systems, and data.

The role of the office worker in an organization's security and privacy is to comply with the company's security policies, avoid circumventing the controls that IT has put in place, and use appropriate channels to communicate their requests for changes to any policies and controls that they think are keeping them from performing their jobs effectively.

Everything is connected in today's corporate environment, and if we all try to help each other do our jobs, then our own work will get done faster and with a lot less hassle.

Dilbert should quit his job and move on with his life.

CHAPTER 2

Alice Downloads a Document

IN THIS CHAPTER, YOU WILL

- Learn how to configure and use Protected View so you can inspect suspicious documents before working on them.
- Learn how to make Microsoft Word remember your decision concerning a document's trustworthiness so that you won't need to make the same decision again later.
- Learn how to designate a folder as a trusted location so that you can work more easily with documents that contain active content.

ALICE works at the head office of Northwind Traders, a large company with dozens of smaller branch locations around the country. Her job is to develop sales proposals for customers and involves working with business documents she often needs to download from different branch offices of the company, from the company's Microsoft SharePoint team sites located in a private cloud hosted at the company's data center, and occasionally from the Internet. Both customers and partners often send her documents via email as well.

Alice uses Microsoft Office applications like Word and Microsoft Outlook for performing many of her job-related tasks. The company recently upgraded all of its PCs at the head office from Office 2003 to the newer Office 2010 platform. Although Alice was happy using Office 2003, management informed everyone that with the rising danger of viruses and other malware infecting the company network through maliciously crafted Word documents, Microsoft Excel spreadsheets, and Microsoft PowerPoint presentations, the company has decided to move everyone at the head office to Office 2010 because of its enhanced security and privacy capabilities. Alice therefore must ensure that she is familiar with those security and privacy features of Office 2010 that may affect how she does her work.

On the other hand, the company is also trying to cut costs, especially at the numerous branch offices, where the number of employees often changes and there is no full-time IT administrator on the premises. So, instead of deploying Office 2010 at these

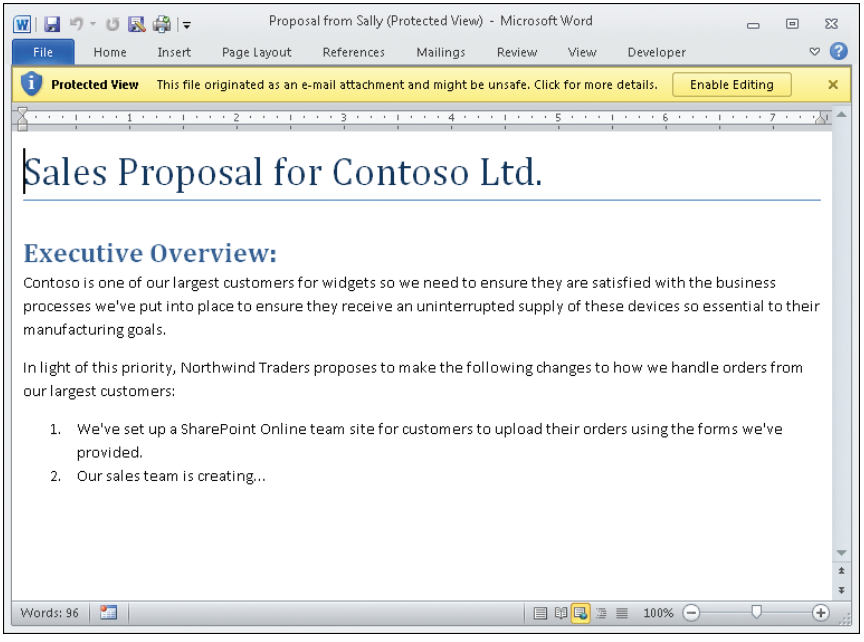
locations, the company has decided to use subscriptions to Office 365 instead so that employees at these offices can use the Office Web Apps to work with documents stored on team sites hosted by Microsoft SharePoint Online. The company thus currently uses a hybrid cloud solution consisting of its own private cloud mainly for the head office, and the public cloud service SharePoint Online for use by its branch offices. Eventually, Northwind hopes to settle on one approach or the other (either private or public cloud), but like many companies today, it's constantly in transition.

Alice also travels from time to time in the performance of her job. When she visits the company's branch locations, she often uses one of their PCs to catch up on her work using Word Web App, so she also needs to be familiar with the security and privacy features available in Word Web App through Office 365.

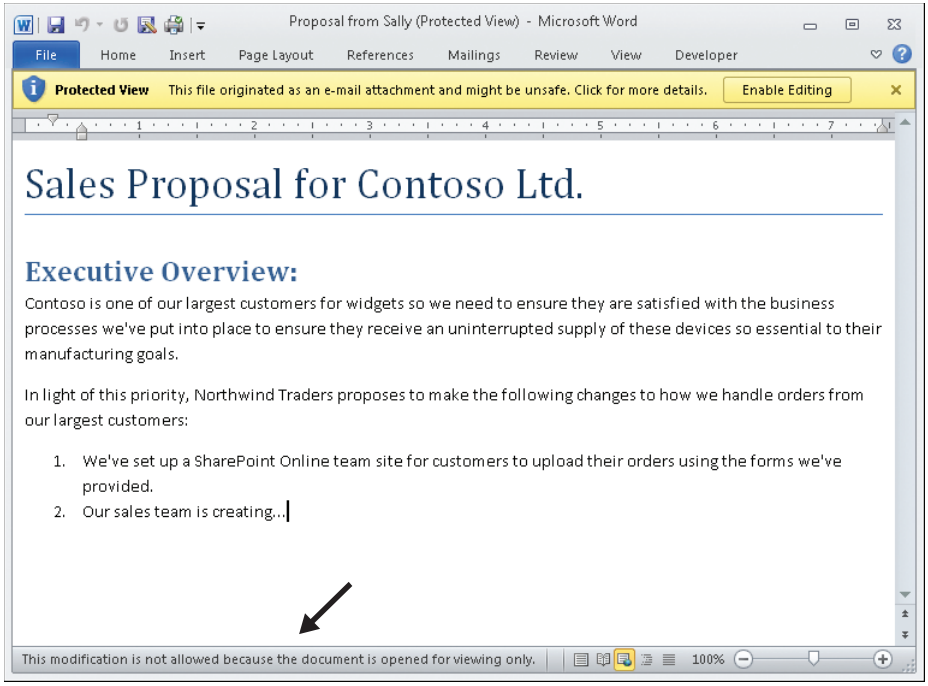
Let's look over Alice's shoulder and watch today as she does her job . . .

Working with Protected View

Sally has just emailed Alice a copy of a sales proposal she's been working on. Alice uses Outlook to download Sally's message from the company mail server. When she tries to open the Word document attached to Sally's message, she sees this:



Being in heads-down busy mode, Alice momentarily ignores the yellow message bar at the top of the document and tries to begin working on finishing the proposal. But when she tries to type text into the document, nothing happens. Then she notices that each time she tries to enter text, a message appears in the Status bar at the bottom of the document as shown:



This finally has Alice's attention. Clearly, the Word document attached to Sally's email can only be viewed, not modified. The reason this is happening is because Word documents attached to email messages in Outlook have some hidden data associated with them. This hidden data is called the file's *zone information*, and it is added by something called the Attachment Execution Services (AES) to indicate that the file came from an untrusted source.

Danger Ahead

When Word 2010 determines that the document you are trying to open comes from an untrusted source, the program automatically opens the document in Protected View. A common metaphor used to describe Protected View is the sandbox. When children are playing in a sandbox, they can safely build castles and destroy them without any impact on the real world around them. In other words, sandboxes are "safe" environments where

kids can play with no problems. Protected View is similar to this because it provides a safe environment where you can view Word documents without worrying about any dangerous content they might contain.

Dangerous content? What kind of dangerous content can Word documents contain? And how often is this a problem? Is it really something that office workers like Alice should worry about?

Absolutely! In 1999, a virus called Melissa emerged and was spread through infected Word documents. When a user opened an infected document attached to an email message, the virus automatically used Outlook to send copies of the document to the first 50 contacts in the user's address book. Once the 50 recipients opened the attached document, the virus replicated itself again, resulting in 50 x 50 = 2,500 emails, and so on. The result of all this was that Internet email systems around the world were quickly overwhelmed and crashed by the flood of messages created by the virus. Since then, numerous other attempts have been made by malicious hackers to use Word documents, Excel spreadsheets, and other Office files to attack corporate networks.

That's one reason why it's so important to be able to understand and properly use the security features of Word and other Office programs. Malicious hackers know that users are often the weakest link in the chain as far as corporate security goes. That's why infected attachments often have alluring file names like ILOVEYOU or seem to have come from a trusted source, like a newsletter service. After all, who wouldn't want to open a file like that?

What kind of dangerous content can a Word document contain? Here are a few examples of potentially dangerous content you should be aware of:

- Hyperlinks that lead users to malicious websites
- Active content such as ActiveX controls, macros created with Microsoft Visual Basic for Applications (VBA), and other forms of executable content.
- Data connections (more common in Excel spreadsheets)

Note that such types of content aren't dangerous per se; it's only when they are maliciously crafted that problems can occur. A maliciously crafted document can even contain executable code that can infect your computer if you simply open the document.

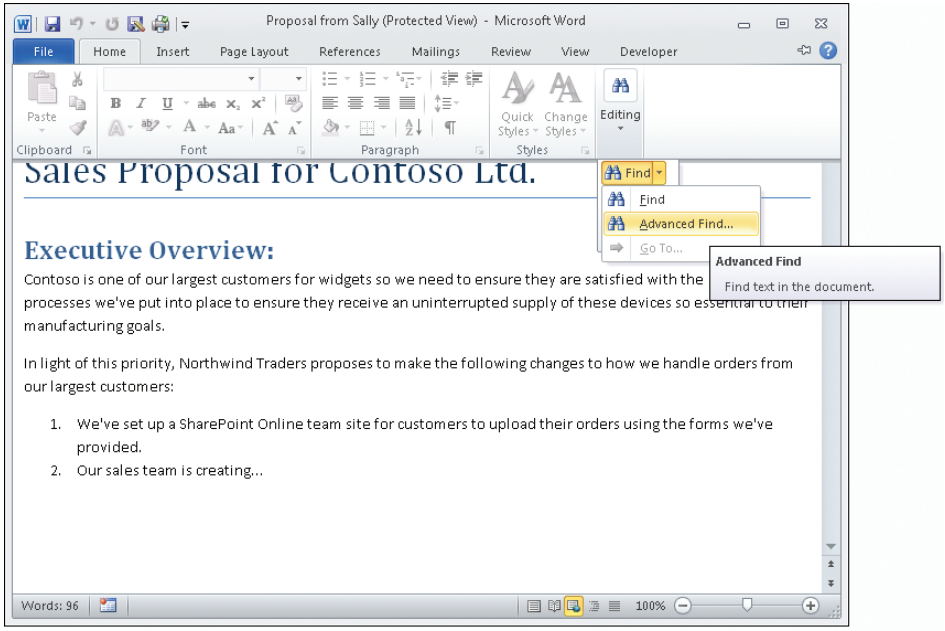
Inside Protected View

The yellow message bar alerts Alice that Sally's proposal has been opened in Protected View. When a document has been opened in Protected View, any malicious content it contains will not execute. For example, if the document contains a macro, the macro will not run.

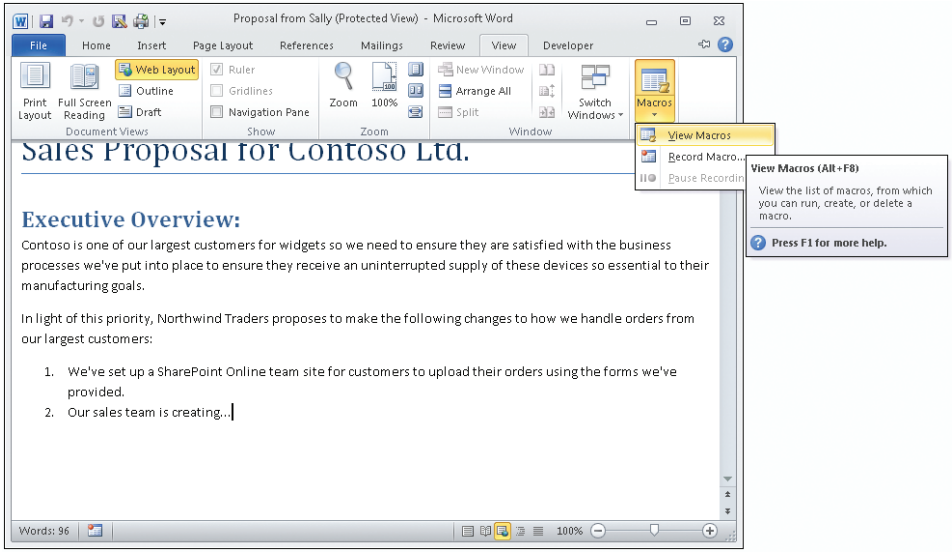
Once the proposal has been opened in Protected View, Alice can scroll through the document to see what's in it. Protected View thus provides a safe read-only environment that allows Alice to inspect the contents of the document. This can be helpful in determining whether the document comes from a legitimate source that can be trusted.

What else can Alice do with a document opened in Protected View? She can copy text from the document and paste it into other programs. This may be useful in situations where there is significant doubt concerning the trustworthiness of the document, because it allows you to extract useful content from the document while leaving the document itself safely in the sandbox.

Alice also can search for text within the document. To do this, she clicks the Home tab on the ribbon and notices that although most of the controls on the ribbon are unavailable (dimmed), the Editing control is available and allows her to select Find or Advanced Find, as shown here:

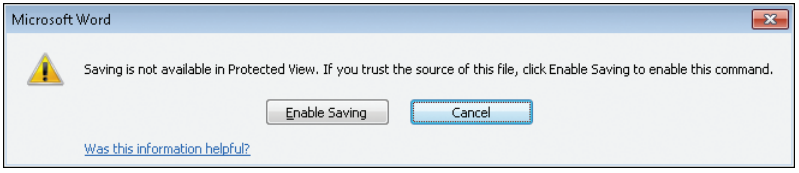


Some of the controls on the View tab on the ribbon are also available. For example, Alice can display a list of macros contained within the document, which may help her evaluate the trustworthiness of the document:

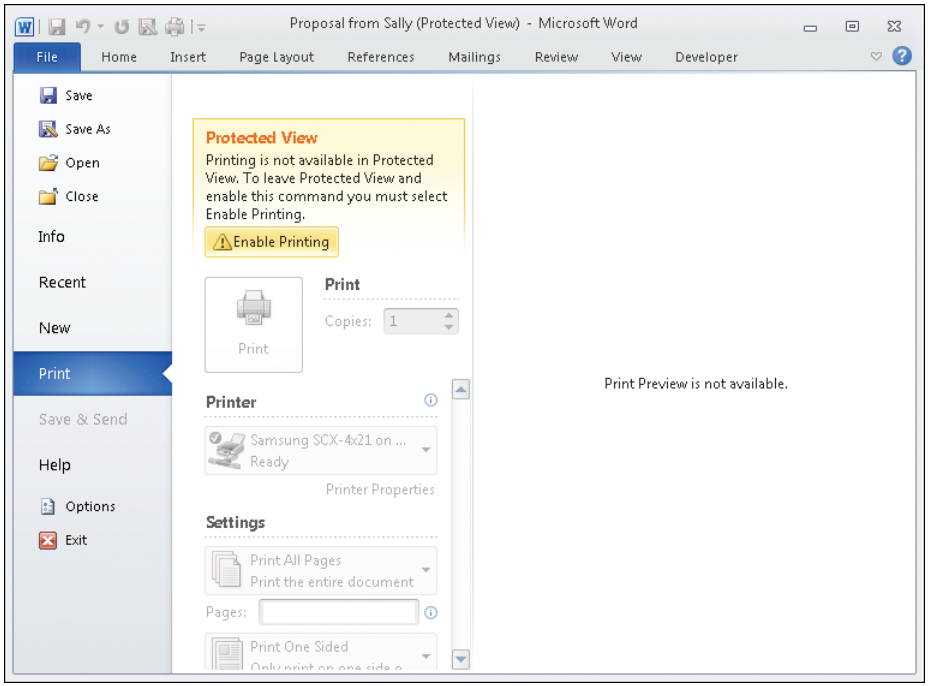


■ **FIVE-MINUTE EXERCISE** **Attach a document to a new message in Outlook and send it to yourself. Once you receive the message, open the attachment in Word. With the document now open in Protected View, explore the ribbon to discover which Word features work in Protected View and which don't.**

After exploring which ribbon controls are available in Protected View, Alice decides to save the document before going any further. She clicks Save on the Quick Access Toolbar at the upper-left corner of the Word window, and this dialog box appears in response:



Protected View doesn't allow you to save documents. The reason is that if the document contains malicious content, you don't want it on your hard drive. Alice then tries to print the document, but this action fails as well, with the following message displayed:

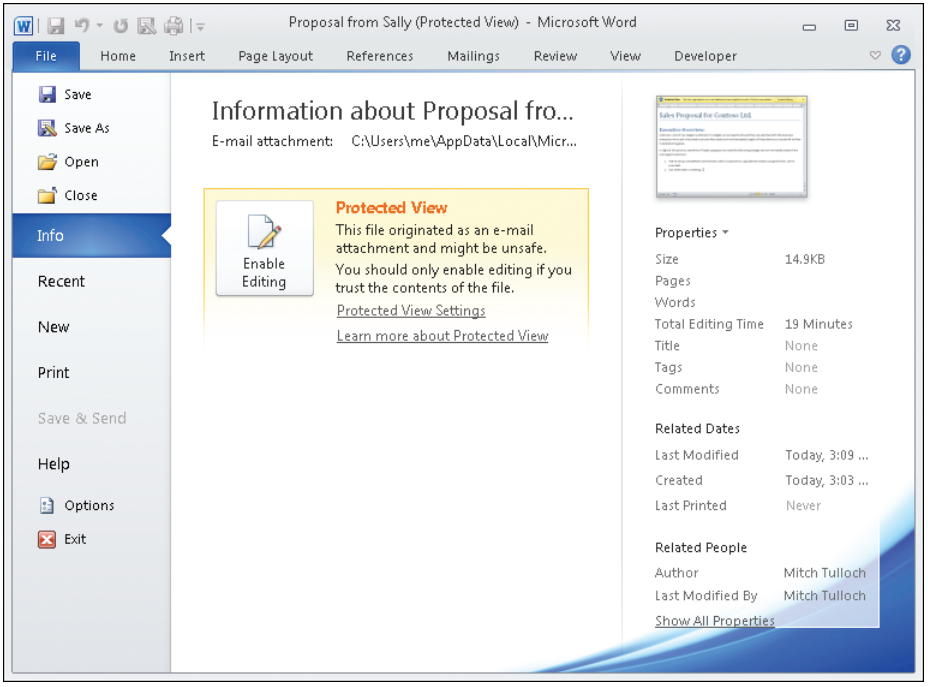


The message displayed above in Backstage View (accessed on the File tab on the ribbon) indicates that you have to leave the sandbox if you want to print the document. The reason for this has to do with how Windows must process documents in order to print them. To minimize the chance of malicious content within a document being executed during the print process, printing functionality is disabled in Protected View.

Tip

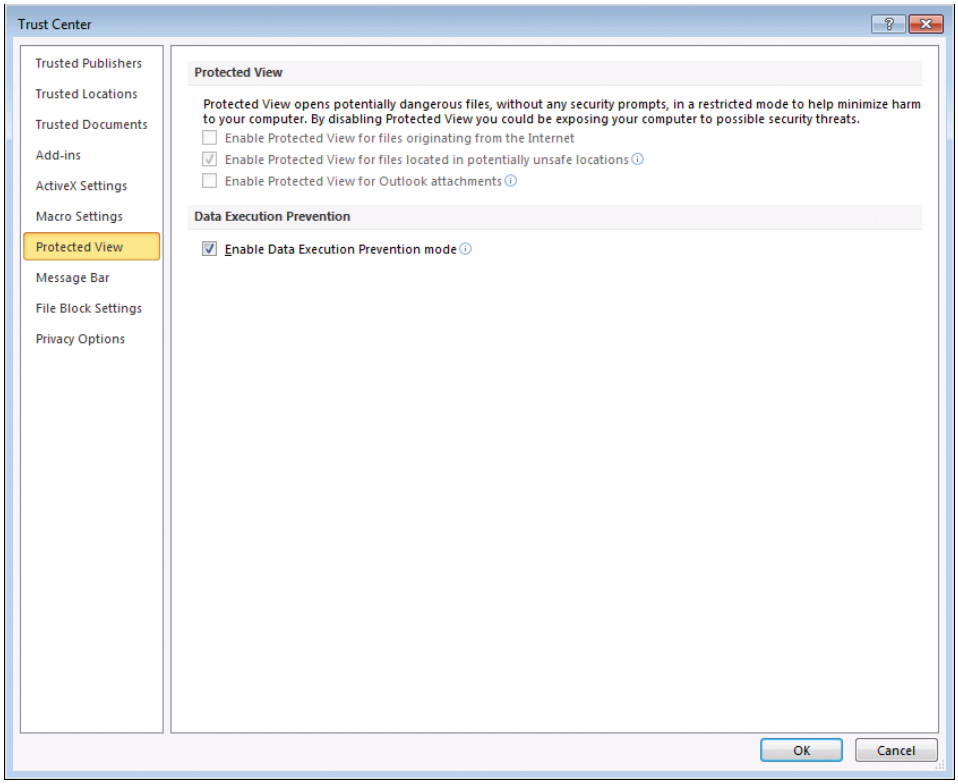
Configuring Protected View

Alice decides to explore Protected View further, so she selects the Info option in Backstage View and clicks the link that says Protected View Settings, as follows:



Doing this opens the Trust Center with the Protected View settings displayed, as shown on the following page:

TIP



Alice wonders why some of the settings for configuring Protected View are unavailable (dimmed), so she calls the help desk. The answer she gets from the staff is that the dimmed settings have been configured by IT and are enforced for all Office users using Group Policy. Alice wonders for a moment whether she should try to circumvent these policies that IT has put in place. What do you think? If you're not sure, refer back to Chapter 1, "Why Should I Care?" and you'll find the answer there.

If Alice were working in an environment where these settings were not enforced by policies that IT put in place, or if her computer were an unmanaged computer (belonging to a workgroup instead of a domain), then she would be able to configure each of the Protected View settings shown above. By default, all three of these settings are enabled when not governed by policy, and best practice is generally to leave them all enabled. Table 2.1 explains what each of these settings means and provides some insight into when you might consider disabling them.

TABLE 2.1 Settings for Configuring the Behavior of Protected View in Word 2010

SETTING	RECOMMENDATIONS
Enable Protected View For Files Originating From The Internet	Documents that you download from the Internet will open automatically in Protected View. Because a lot of malware is floating around on the Internet, it's usually best to leave this setting enabled. If you choose to (or are allowed to) download documents only from trusted websites, then you could consider disabling this setting. If you do so, however, make sure that the antivirus software on your computer is up to date, just in case. And if you're sure a downloaded document can be trusted, you also can remove the "from the Internet" part from a downloaded document manually by opening the document's properties in Windows Explorer and clicking Unblock.
Enable Protected View For Files Located In Potentially Unsafe Locations	Certain folders, such as where Windows stores downloaded programs and the Temporary Internet Files folder used by Windows Internet Explorer, are considered potentially unsafe locations. As a result, when the user tries to open a document stored in these locations, the document opens in Protected View. Also, your administrator can designate additional folders, either on your computer or on the network, as potentially unsafe locations. If you frequently access documents stored in a specific folder or network share and find that they always open in Protected View, and if you consider this an unnecessary inconvenience, you might consider asking your administrator to remove the folder/share from the list of potentially unsafe locations determined by Group Policy.
Enable Protected View For Outlook Attachments	Documents attached to email messages you receive via Outlook and try to open in Word are opened automatically in Protected View. Because email can sometimes be spoofed, a message that you think you've received from a colleague may actually have originated from someone with malicious intent. And sometimes a colleague might accidentally send or forward you a document that they think is harmless but is in fact maliciously crafted. Because of this, it's a good idea to always leave this setting enabled. If you are not using Outlook as your email client, you could consider disabling this setting, but there is no real benefit gained from doing so.

■ FIVE-MINUTE EXERCISE **Besides Word, two other Office 2010 programs (Excel and PowerPoint) also use Protected View. How are the Protected View settings in the Trust Center for these two applications similar to those for Word? How are they different?**

OFFICE 365 AND PROTECTED VIEW

At the time of writing, Word Web App does not support Protected View. This means, for example, that if Alice is logged onto Office 365 and uses Word Web App to try to open a document attached to an email message she received using Outlook Web App, the document will open normally for editing in Word Web App. And if she tries to open a document that has been downloaded from the Internet and uploaded to the Northwind Traders team site in SharePoint Online, the document will again open normally for editing in Word Web App.

In other words, the Office Web Apps included in your Office 365 subscription don't have the same security and privacy capabilities that the full Office 2010 suite of programs has. However, this doesn't mean that Office 365 isn't secure, for it's extremely secure on the cloud side. In fact, Protected View is less critical in Office Web Apps because your documents, spreadsheets, and presentations aren't being rendered by Office programs; instead, they're being rendered by Internet Explorer.

For example, even though you can open Word documents that contain macros such as .docm or .dotm files using Word Web App, the macros in the document will not run. ActiveX controls will display as expected in Reading View with Word Web App, but in Editing View, they only appear as placeholders that you can delete but not edit, move, or resize. And you can even customize your Internet Explorer security settings to prevent ActiveX controls from loading if desired (your administrator also can use policy to enforce this).

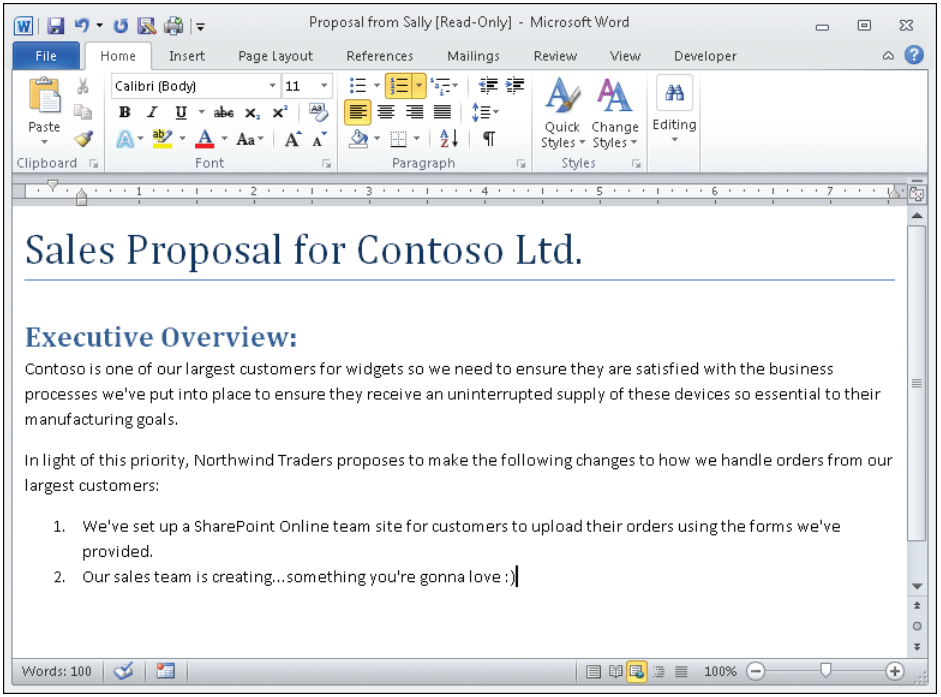
See Also If you're interested in learning more about how Microsoft ensures the security of its Office 365 offerings, you can read the "Security in Office 365" white paper available from the Microsoft Download Center at *http://www.microsoft.com/download/en/details.aspx?id=26552*.

Exiting Protected View

Alice feels confident that the proposal from Sally that she has open in Protected View can be trusted, so she decides to exit Protected View so she can continue to work on the proposal. There are several ways she can do this:

- She can click Enable Editing on the yellow message bar above the document.
- She can click Enable Saving if she had just tried saving the document to her hard drive.
- She can click Enable Printing if she had just tried printing the document.

Regardless of the method Alice chooses, once the document exits Protected View, she can edit it, save it, or print it as needed:



This raises a question, however: How can Alice be sure the document that Sally sent her can be trusted? There's no hard and fast answer to this, but here are some guidelines that may help you decide whether to enable editing for a document opened in Protected View:

- You trust the individual(s) who created and/or sent you the document, and you know that they have up-to-date antivirus software on their computers.

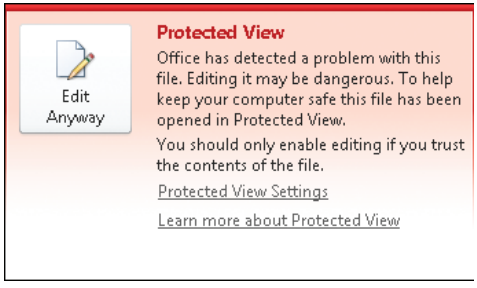
- You also have up-to-date antivirus software on your computer and, if necessary, you have run an antivirus check against the document manually.
- You've scrolled through the document and nothing appears strange or out of place in it. You've also used the View tab on the ribbon to see if the document contains any macros and there are none present.
- You have your fingers crossed.

If all of the above are true (well, may be the last one isn't strictly necessary), you probably can go ahead and enable editing for the document—unless, of course, management has provided you with different instructions in the corporate security policy concerning documents that open in Protected View. For example, management might decree that "Users must immediately notify the help desk when a document they receive opens in Protected View, and they must not enable editing for the document unless advised to do so by the help desk." Remember, when in doubt, follow the rules.

Other Triggers for Protected View

Trying to open a document attached to an Outlook email you received isn't the only scenario that will trigger Word to open a document in Protected View. For example, someone later gave Alice a USB flash drive containing some older Word 2003 documents; that is, they were .doc files as opposed to the newer .docx file format that Word 2007 and Word 2010 use by default. When Alice tried to open one of these older .doc files in Word, the following red message bar was displayed:

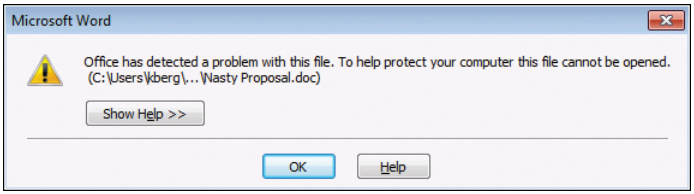
Clicking this message bar opens Backstage View, where the following is displayed:



Should Alice click Edit Anyway and exit Protected View so she can edit the document? Generally, the answer in this kind of situation should be "no." That's because what's likely happened here is that the older .doc file failed what is known as Office File Validation,

which means that the structure of the document doesn't conform to the standard rules for the .doc file format. This could be because the document accidentally became corrupted somehow, and Word might be able to repair it if you tried to open it. But it also could be because the document has been maliciously tampered with; for example, someone may have inserted hidden executable content within it that can wreak havoc on your computer, or even the entire corporate network. So, in general, when you see this kind of red message bar, you should avoid exiting Protected View and contact the help desk staff instead so they can investigate further. At best, you might use copy and paste to copy content from the corrupt document into a new document so that you can use the content in the corrupt document if needed.

In some environments, when you try to open a .doc file that fails validation, instead of seeing the red message bar, you see a dialog box like this:



This occurs when your administrator has configured Group Policy to prevent users from opening files that fail validation even in Protected View. The administrator has likely done this because of security concerns, so you shouldn't try to find a way to circumvent this control.

If you download a document from a website on the Internet and then try to open the document in Word, it may open in Protected View and display a message bar like this:

If for some reason your administrator has disabled the "Enable Protected View for files originating from the Internet" policy described earlier, then this won't occur. Instead, the downloaded document will open normally in Word and can be edited immediately.

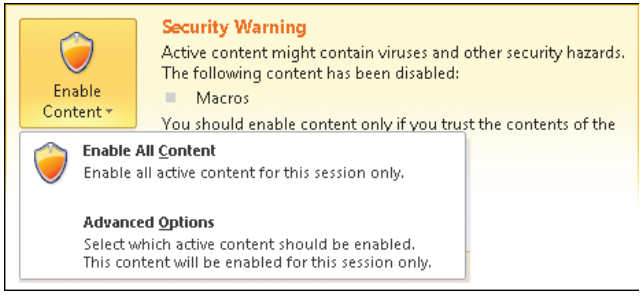
Understanding Trust

If a document opens in Protected View and you decide to exit Protected View so that you can edit the document, this may not be the end of the matter as far as security goes. For example, when Alice enabled editing for Sally's proposal, the document

exited Protected View and then could be edited. But if Sally's proposal also happened to contain some macros (and your administrator has configured macro security accordingly), then Alice might have seen a second yellow message bar like this:

Although the document now can be edited by Alice, any macros in it will not execute unless she enables macro functionality in the document. Alice can do this in two ways. First, she can simply click Enable Content in the above message bar to enable all macros within the document. Second, she can click the File tab on the ribbon to display Backstage View, which shows the following:

Clicking Enable Content displays two options, allowing Alice either to enable all active content in the document or to enable only selected active content:



If Alice chooses the second option, Word displays an additional dialog box that offers further options for dealing with macros in the document, as shown on the following page:

Similar message bars, Backstage options, and dialog boxes are displayed if the document contains other types of active content, such as add-ins or ActiveX controls.

Trusted Documents

If Alice decides to enable active content in the document, Word considers her action to be a "trust decision" and saves a record of her decision in the registry on her computer. This way, the next time Alice attempts to open the same document, Word "remembers" that Alice previously decided to trust the active content in the document and automatically enables macro functionality in the document. In other words, Alice only sees the above security warning once if she decides to click Enable Content on the yellow message bar. If she decides not to click Enable Content, then no trust decision has been made on her part, and the next time she attempts to open the document, Word once again displays the security warning. Note that the Advanced Options for enabling active content enable such content only for the current session—that is, until the document is closed.

This feature of the Office 2010 applications Word, Excel, PowerPoint, Microsoft Access, and Microsoft Visio is known as Trusted Documents, and it can be configured from the Trust Center as shown on the next page (provided your administrator hasn't used Group Policy to block you from changing these settings):

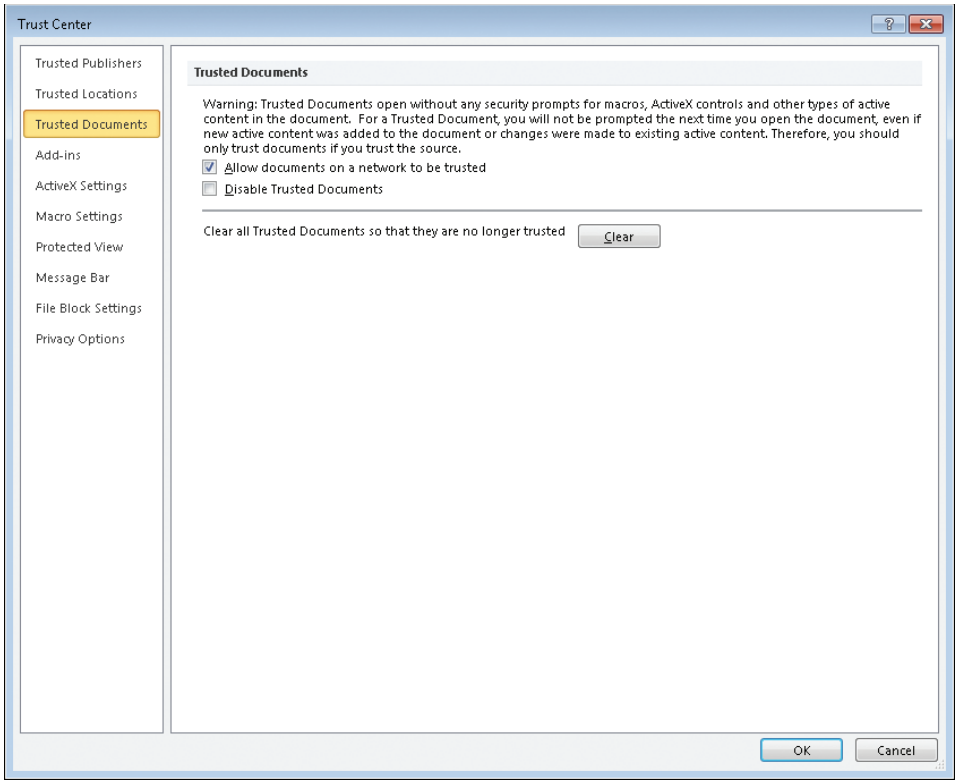


Table 2.2 explains what each of these settings means and explains how you might want to configure them (if your administrator allows this).

TABLE 2.2 Settings for Configuring the Behavior of Trusted Documents in Word 2010

SETTING	RECOMMENDATIONS
Allow Documents On A Network To Be Trusted	Trust decisions will be remembered for documents stored on network shares. This setting is enabled by default unless overridden by policy. If the administrator has configured access control permissions properly for the shared folder, and if you trust the other users who have access to this share, you could consider leaving this setting enabled if policy doesn't prevent you from doing so. If you disable this setting, the yellow message bar will be displayed whenever the user attempts to open a document stored in the shared folder.

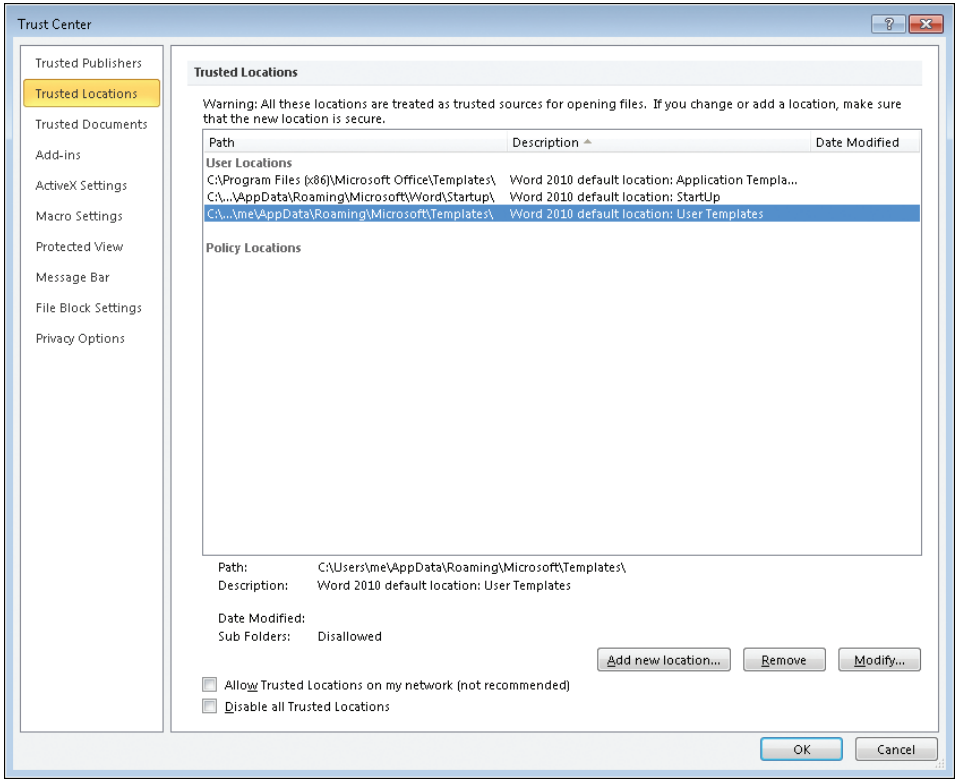
SETTING	RECOMMENDATIONS
Disable Trusted Documents	Trust decisions will not be remembered. The result is that the yellow message bar is displayed each time the user attempts to open the document. This setting is disabled by default unless overridden by policy. If you are concerned about the possibility of unanticipated active content being present in documents you work with, you could consider enabling this setting. Doing this will cause the yellow message bar to be displayed each time the user attempts to open any document. However, this approach tends to be ineffective from a security standpoint because eventually users get accustomed to just clicking Enable Editing whenever they see a yellow message bar, without even bothering to read the message bar.
Clear All Trusted Documents So They Are No Longer Trusted	Clicking this button clears all trust decisions the user previously made from the registry. You could consider doing this when you are finished with a big project and ready to start another. The reason is that only a limited number of trust decisions can be remembered, so clearing the list of Trusted Documents makes room for new trust decisions to be remembered.

Trusted Locations

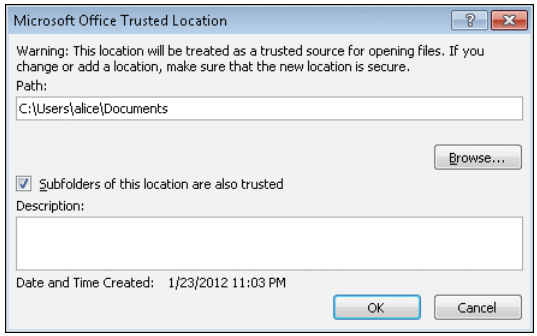
Another aspect of trust in Office 2010 applications is the feature known as Trusted Locations. This feature is available in Word, Excel, PowerPoint, Access, Visio, and Microsoft InfoPath. Users can specify trusted locations on a per-application basis from within the Trust Center, whereas administrators can use Group Policy do this and also specify trusted locations on a global basis for all supported Office applications.

A trusted location is basically a folder designated in such a way that any documents it contains are trusted. In other words, if you use Word to open a document stored in a trusted location, the document is opened for editing and *all* active content in it is enabled. Clearly, trusted locations are powerful and shouldn't be abused. You must make sure that only appropriate content (content you believe is trustworthy) is stored in such locations.

Trusted locations can be either folders on your hard drive or shared folders on the network. By default, shared folders on the network cannot be trusted unless the user selects the Allow Trusted Locations On My Network (Not Recommended) checkbox, as shown below. Also by default, only certain folders used by Word are configured as trusted locations, specifically the default startup location for Word and some folders where templates are stored:



Let's say that Alice decides to add a new trusted location, namely her Documents folder and any subfolders of this folder. She takes this step so that any documents she has saved in her Documents folder or its subfolders will open for editing automatically, with all active content enabled. Because Alice is careful what documents she saves in her Documents folder, she thinks this is an appropriate action for her to take. To do this, Alice clicks Add New Location in the Trusted Locations panel of the Trust Center shown above. Doing this opens a dialog box that lets her specify the folder she wants to designate as a trusted location and whether to include subfolders in her trust decision, as shown on the next page:



As with all security options in Office 2010 programs, users may be blocked from changing these settings if the administrator of the network has used Group Policy to enforce a desired configuration of settings.

BEST PRACTICES FOR CHOOSING TRUSTED LOCATIONS

What are some best practices for choosing possible locations to be trusted? Here are some guidelines you may want to consider.

If you work with large numbers of documents that contain active content, it might be a good idea to designate a folder on your computer as a trusted location and store your documents in this location. This way, you won't see the yellow message bar the first time you open any of these documents. Be careful, however, to include only documents you believe you can trust. For example, if you work alone with these documents and create all the macros in them, you are probably safe.

Documents stored in trusted locations are not validated before Word opens them. This means that if there happens to be a maliciously crafted .doc file in such a location and you try to open it, your computer could become infected in some fashion. So make sure that you store only newer .docx or .docm files in a trusted location and not older .doc files.

Specify a shared folder on the network as a trusted location only if access to the shared folder has been properly secured using NTFS permissions.

In general, don't designate your Documents folder as a trusted location (as Alice did) because it's just too easy to save a document you don't want in that folder accidentally. Instead, create a subfolder (or tree of subfolders) within your Documents folder and designate the subfolder (and, optionally, the folders beneath it) as a trusted location.

Don't designate the root folder C:\ as a trusted location. You don't ever want to store documents or anything else in your root folder.

You also can designate SharePoint sites as trusted locations, although it's likely that your administrator will do this for you.

Summary

Protected View provides a safe "sandbox" environment that lets you read, search, and even copy and paste from documents while preventing you from saving or printing them or executing any active content within them.

Trusted Documents allows users' decisions concerning the trustworthiness of a document to be remembered so that next time they open the document, any active content within it execute automatically.

Trusted Locations enables the user to designate a specific folder on the computer's hard drive or on a network file server as containing only trusted content.

Users can use the Trust Center to configure how Protected View, Trusted Documents, and Trusted Locations works on their computer. Administrators can override users' Trust Center settings and enforce a different set of settings using Group Policy.

Only certain Office 2010 applications have the Protected View, Trusted Documents, and Trusted Locations features. The Office Web Apps included with Office 365 do not currently have these features.

CHAPTER 3

Bob Prepares a Policy

IN THIS CHAPTER, YOU WILL

- Learn how to remove private information from a Microsoft Word document that you need to prepare for publication or sharing with others.
- Learn how to sign a document digitally so the recipient can be sure it's from you and hasn't been altered.
- Learn how to mark a document as final so it can't be modified by others.

BOB WORKS in Alice's department at the head office of Northwind Traders. Bob's role is to create drafts of content being developed for the organization's customers, and Alice reviews Bob's content prior to distributing it to customers.

Bob has been working on creating a new privacy policy for Contoso Ltd., a major customer of Northwind Traders. Bob is relatively new to working with Microsoft Office, and as part of his orientation training by Human Resources, Bob was informed about the importance of removing all sensitive or proprietary company information from documents prior to distribution to customers. Bob also was informed that all content created for customers must be signed electronically by the content's creator and that the creator's manager also must electronically sign off on the content as part of the review process for ensuring the readiness of the content for distribution. Finally, Bob also was informed that all content distributed to customers must be marked as final so it can no longer be altered in any fashion.

To ensure that Bob can perform his work role correctly, Alice walks him through the process of inspecting the policy he's been working on for internal company information, removing any such information that might be found, digitally signing the policy and preparing it for Alice to countersign, and ensuring that the final policy is read-only. While Alice uses Word 2010 for performing this walkthrough with Bob, she also explains the differences that Bob would encounter if he used the Word Web App of Office 365 for this process.

Understanding Document Properties

When you use Word to create or modify a document, Microsoft Excel to work on a spreadsheet, and so on, the Office program you use may add certain kinds of hidden information to the document automatically. This hidden information is called *document properties,* and it may include such things as:

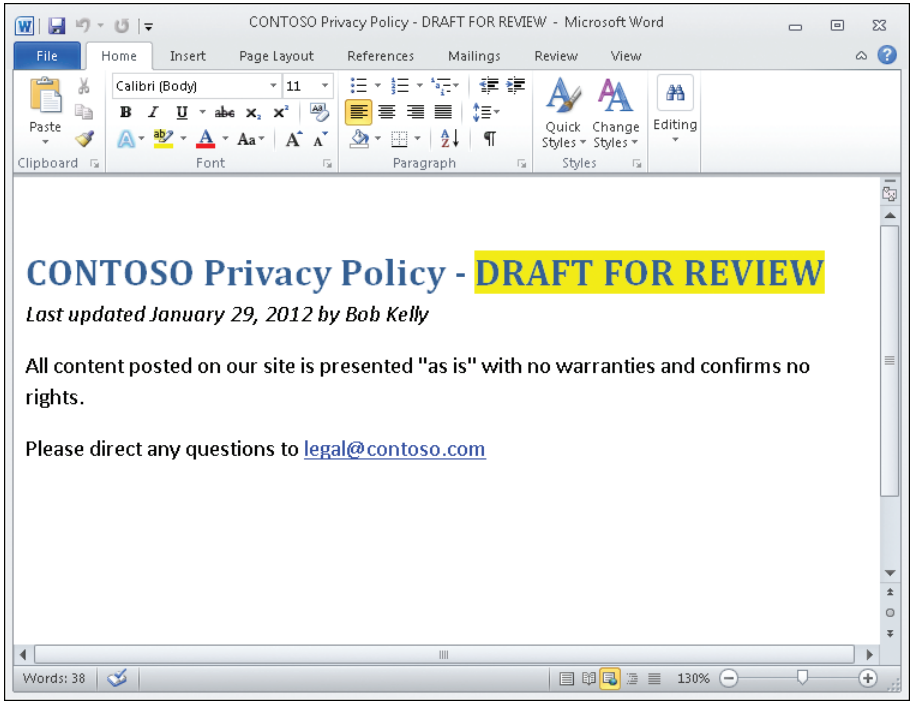
- The name, title, manager's name, and other identifying information about the author of the document
- The date that the document was created or modified
- Any custom properties that you decide to create and assign to the document for different purposes
- Other properties relating to your organization or to the document library in which the file is stored

Some document properties, like Date Last Modified, are inserted automatically by Office, and you can't modify them. Other properties, like Author, are inserted by Word but you can edit them (you can even add more names to have multiple authors for a document). And when you add a new custom property to a document, you can either select it from the default list of custom properties, which includes things like Date Completed and Checked By, or you can even define your own custom properties, such as For Sharing With Customer.

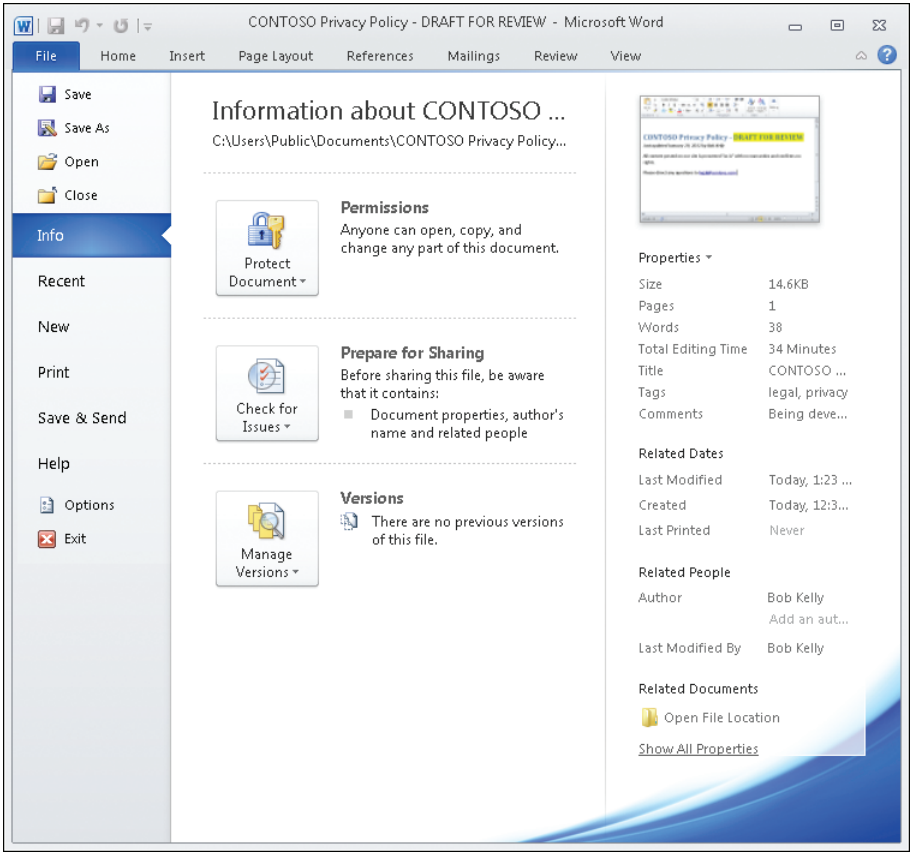
The important thing to remember as an office worker is that some document properties contain internal information about your company, such as your title as an employee or your manager's name, and your company's privacy policy likely prohibits the inclusion of such information in documents shared with customers, exchanged with business partners, or published on the Internet.

But before we look at how to find and remove such hidden information or metadata, let's first examine how document properties can be exposed and modified in Office programs like Word.

Bob is working on his draft version of the privacy policy for Contoso. He opens the document in Word as follows:

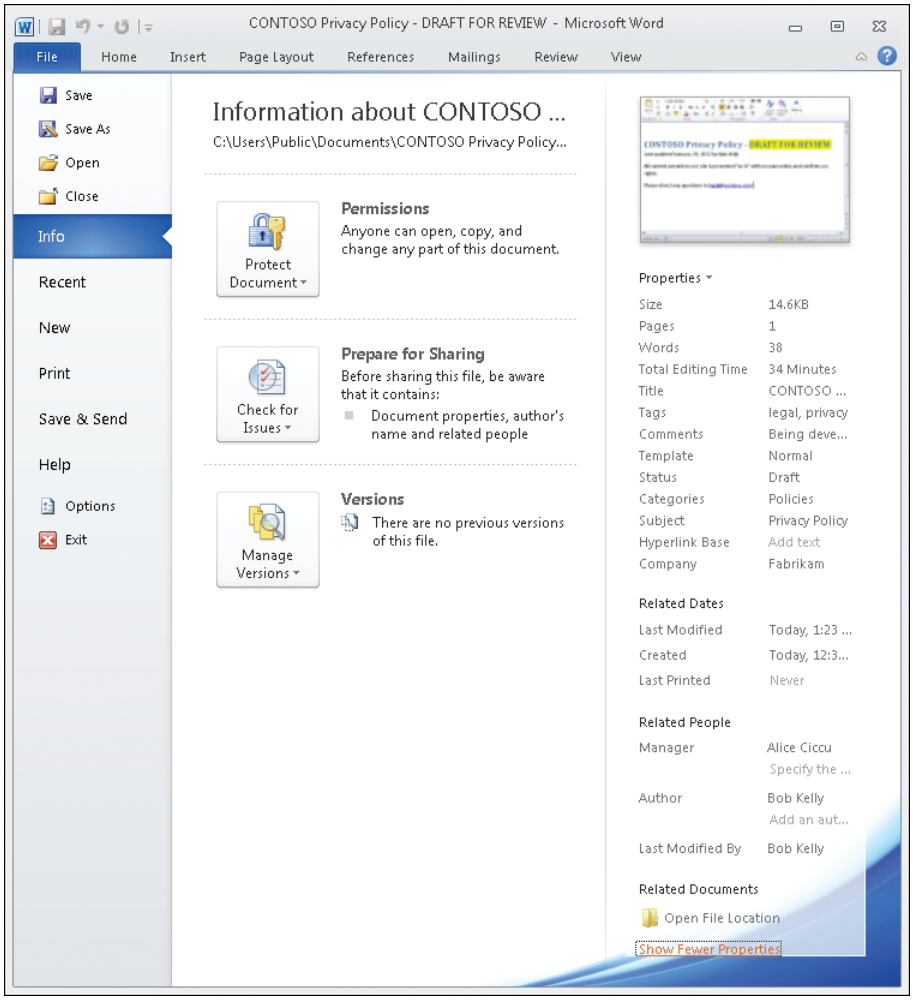


Remembering what the woman in Human Resources told him about removing any sensitive company information from documents he's working on, Bob decides to look at what document properties are currently present in the document. He begins by selecting the File tab to switch the focus of Word to Backstage View, as follows:

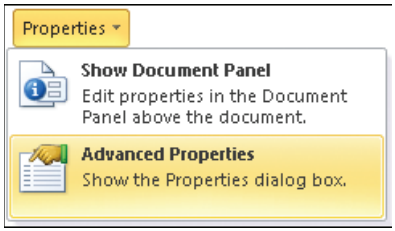


With the Info option selected in the left pane, Bob examines the document properties listed on the right side of Backstage View. He notices properties like Size, Pages, Tags, Comments, Last Modified, Author, and so on.

Wondering whether there might be other properties hidden in the document, Bob clicks Show All Properties at the bottom of the right side of the Backstage View. Doing this displays additional hidden information such as Subject, Manager, and other properties.



Bob still wonders whether there are any other properties hidden in the document. So he clicks Properties under the thumbnail image at the top of the right side of Backstage View. This displays two options he can select from:

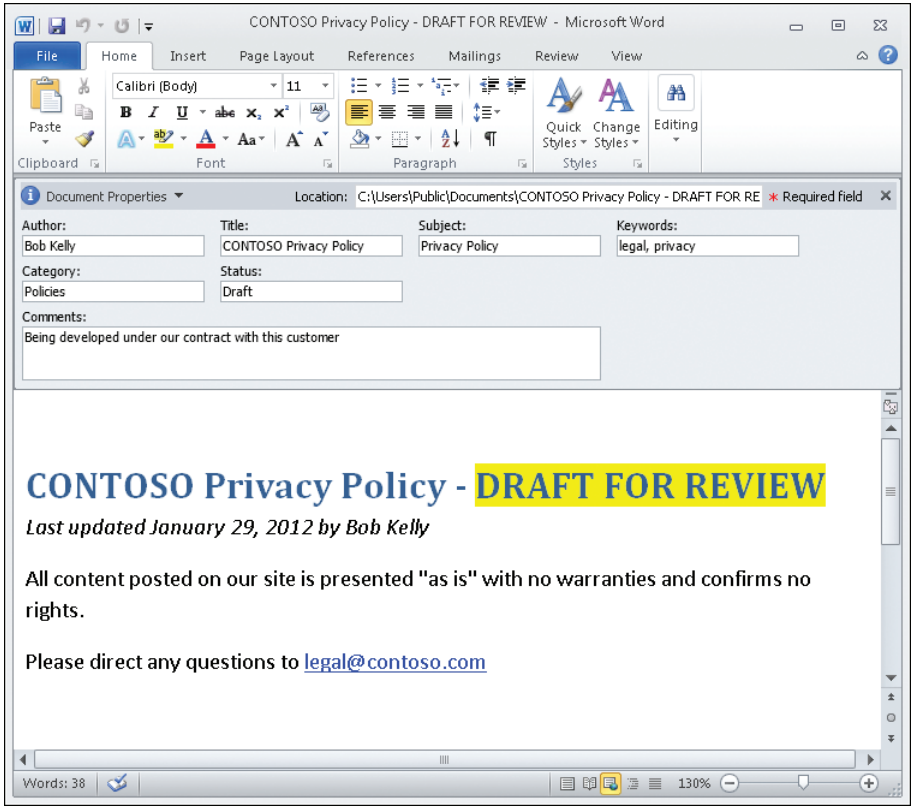


Bob selected the Advanced Properties option, which opens a new window with several tabs:

Bob notices that he can edit the information on the Summary tab of this window, and he is tempted to do this to delete all the information shown on this tab. But then he thinks that there might be an easier way to clean the properties from a document to make it ready for sharing with the customer. He makes a note in the To Do List in Microsoft Outlook to remind himself to ask his manager, Alice, about this later.

■ **Five-Minute Exercise** **Open the Advanced Properties in a few documents, spreadsheets, presentations, and other Office documents and examine the different tabs to see what properties have values set for them. What properties are the most important to specify when working with Office documents in your own work environment?**

Meanwhile, Bob is still wondering about the other option he could have selected when he clicked Properties in Backstage View (Show Document Panel), so he makes this selection to see what it does. Word automatically switches the focus back to the Home tab and opens a new pane called the Document Panel immediately beneath the ribbon as follows:

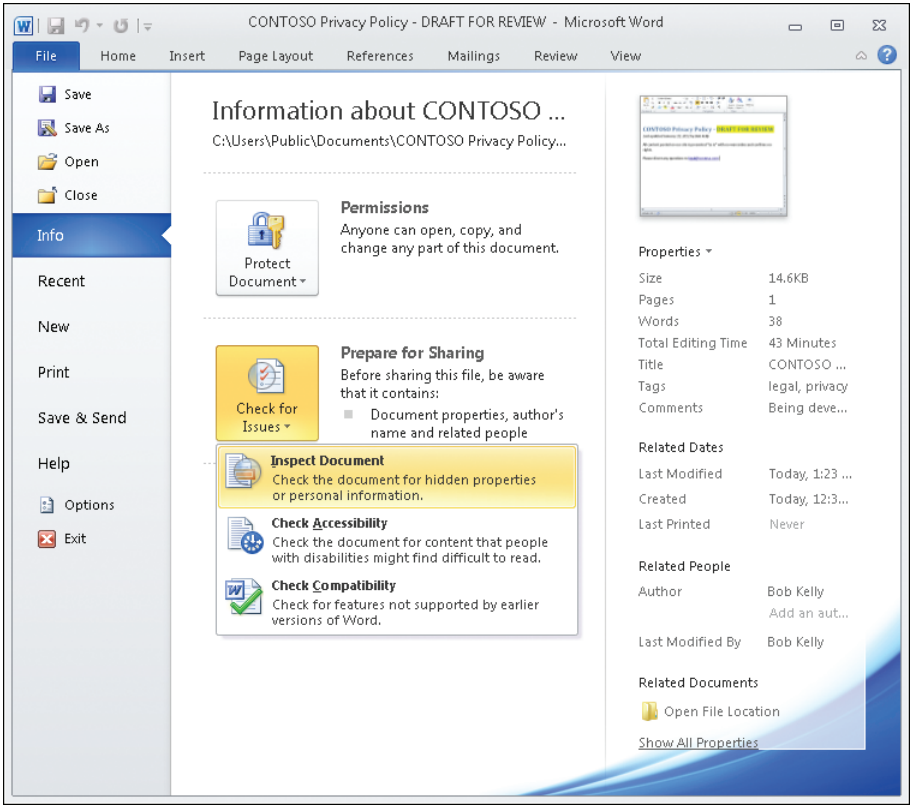


Bob sees that this panel can be very useful because it allows him quick access to viewing or modifying some of the key properties of a document. Therefore, he uses Microsoft OneNote to make some quick notes about the new Word functionality that he has just learned. At this point, the Outlook reminder that he created previously opens, so he sends Alice an instant message using Lync to ask her if she's free to come and show him how to clean the properties from a document.

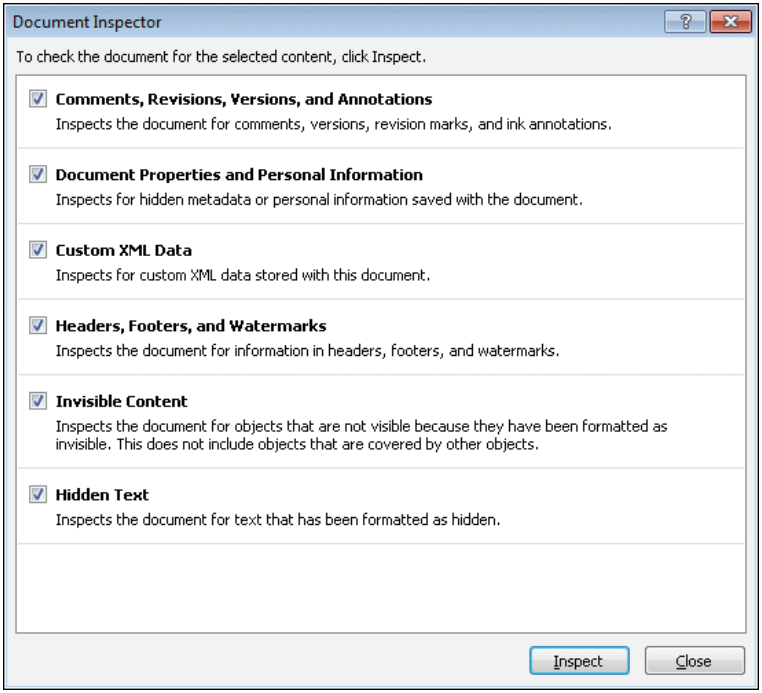
> You may have noticed a red asterisk with the text "Required Field" beside it in the upper-right corner of the Document Panel. Required fields are typically configured by your administrator in a Microsoft SharePoint or Microsoft InfoPath environment and can be used to make sure that users specify values for certain properties before a document can be saved to a SharePoint team site or when using InfoPath forms. Document properties that have been configured as required fields (such as in a SharePoint document library) are then flagged with a red asterisk beside them to indicate this.

Working with Document Inspector

After receiving some quick instruction from his manager, Alice (who is also his company-assigned mentor), Bob decides to use Document Inspector to remove all hidden properties from his document. Bob begins by switching to Backstage View. He then clicks Check For Issues and selects Inspect Document, as shown here:



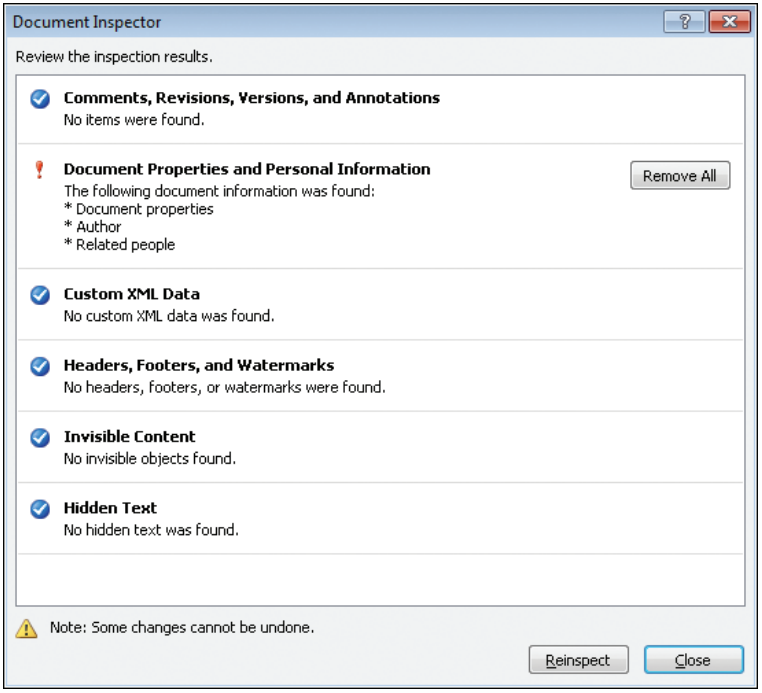
This opens the Document Inspector, as shown here:



In Word 2010, the Document Inspector can find and remove the following kinds of information from a document:

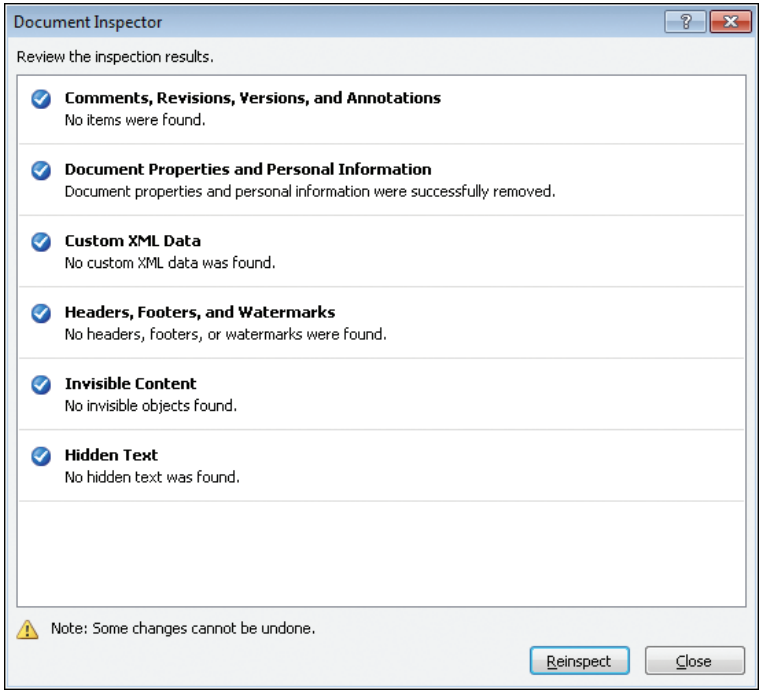
- Markups such as comments, revision marks, annotations, and so on. Such information is commonly added when documents go through a review process involving several different people.
- Document properties, as described in the previous section of this chapter.
- Extraneous XML data in the document that isn't used by Word for formatting purposes or macros. This might happen, for example, if the document was opened, modified, and saved using a program that is not part of the Office suite.
- Headers, footers, and watermarks. Sometimes you want such information to remain in a document you publish, however, so in that case, you would clear the check box for this option.
- Any text or other content contained in the document that has been deliberately formatted as hidden. It's usually not a good idea to hide things in a document in case you forget later that you hid them.

Bob leaves all check boxes selected in the Document Inspector and clicks Inspect to check the document. The result is shown here:

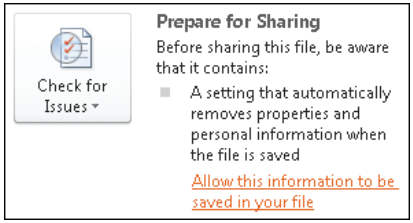


You can't inspect a document unless it's been saved first.

Because of company policy, all document properties and personal information need to be removed before distributing documents to customers, so Bob clicks Remove All to do this. Document Inspector now indicates that the document contains no hidden data or personal information:



After closing the Document Inspector, Bob notices that the Prepare For Sharing control in Backstage View now displays the following text:

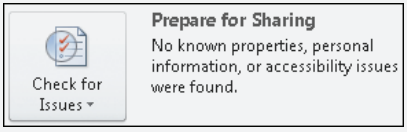


What has happened is that clicking the Remove All button in the Document Inspector caused Word to enable a special setting in the document so that personal information won't be re-entered into the document's properties accidentally when the document is re-saved. The way that you do this in Word is by enabling the Remove Personal Information From File Properties On Save setting, which can be found in the Trust Center Settings under Privacy Options. Therefore, the text "A setting that automatically removes properties and personal information when the file is saved" shown here simply informs the user that this special setting is now turned on.

At this point, Bob saves the document, and the Remove Personal Information From File Properties On Save setting ensures that no personal information about Bob will be saved within the document. When the next person to handle the document opens it and switches to Backstage View, the Last Modified By property will show a Not Saved Yet message instead of displaying the name of the person (Bob) who last saved the document. Bob has finished preparing the document and is now ready to sign it and then send it to Alice for review.

BE CAREFUL WHAT YOU CLICK!

What would have happened if Bob had clicked the Allow This Information To Be Saved In Your File link instead of saving the document? In that case, the Remove Personal Information From File Properties On Save setting would have been disabled for the document, and the Prepare For Sharing control would now display the following text:



At that point, if Bob had saved the document and then he or someone else later reopened it, the Last Modified By property would have shown Bob's name as the last person who had saved the document, which would have meant that some of Bob's personal information (that is, his name) would have been saved within the document. Of course, this is not what Bob would have wanted—he really wanted to send a clean document to the customer.

What's the lesson here? After you run the Document Inspector to prepare a document for sharing with others outside your organization, don't click the Allow This Information To Be Saved In Your File link unless you still have further work to do on the document.

■ **Five-Minute Exercise** **Use the Document Inspector to check some documents, spreadsheets, and presentations that your business has prepared for distribution to customers or business partners. Do any of these Office files contain sensitive or proprietary information about your business that shouldn't have been shared with others? What should you do if you discover this to be true?**

Working with Digital Signatures

A *digital signature* is the digital equivalent of a handwritten signature. You typically sign a Word document, an Excel spreadsheet, or a Microsoft PowerPoint presentation digitally for the same kinds of reasons you might use a pen to sign a paper contract—namely, to confirm that you have read and agree with its content.

Digitally signing a Word document does three things:

- It ensures the authenticity of the document by confirming that the signer is who he or she says.
- It confirms the integrity of the document; that is, it proves that the document hasn't been tampered.
- It ensures non-repudiation; that is, the individual who signed the document can't pretend he or she didn't sign it. The ink is on the hands, as it were.

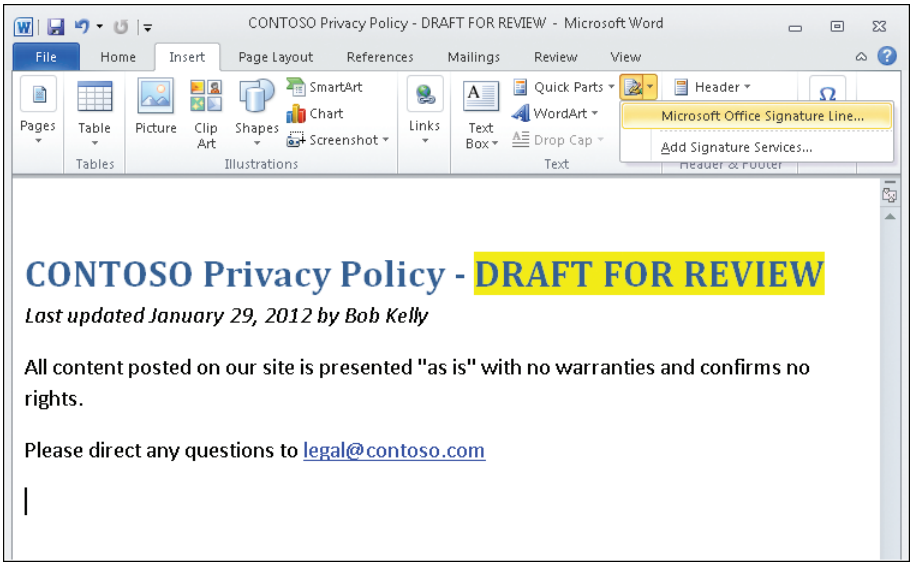
To sign a digital signature, first you must have a valid digital certificate. Digital certificates can be obtained in three ways:

- From a commercial certificate authority (CA), such as the ones you can find through the online Office Marketplace
- From an internal CA that has been set up and configured by your company's IT department
- By creating your own self-signed certificate (recommended for testing purposes only)

In most cases involving office workers, the IT department already will have issued your user account a digital certificate so that you can sign documents, email messages, and other content you work with. If you're interested in obtaining a commercial certificate or self-signing one of your own, see the appendix, "Where to Learn More."

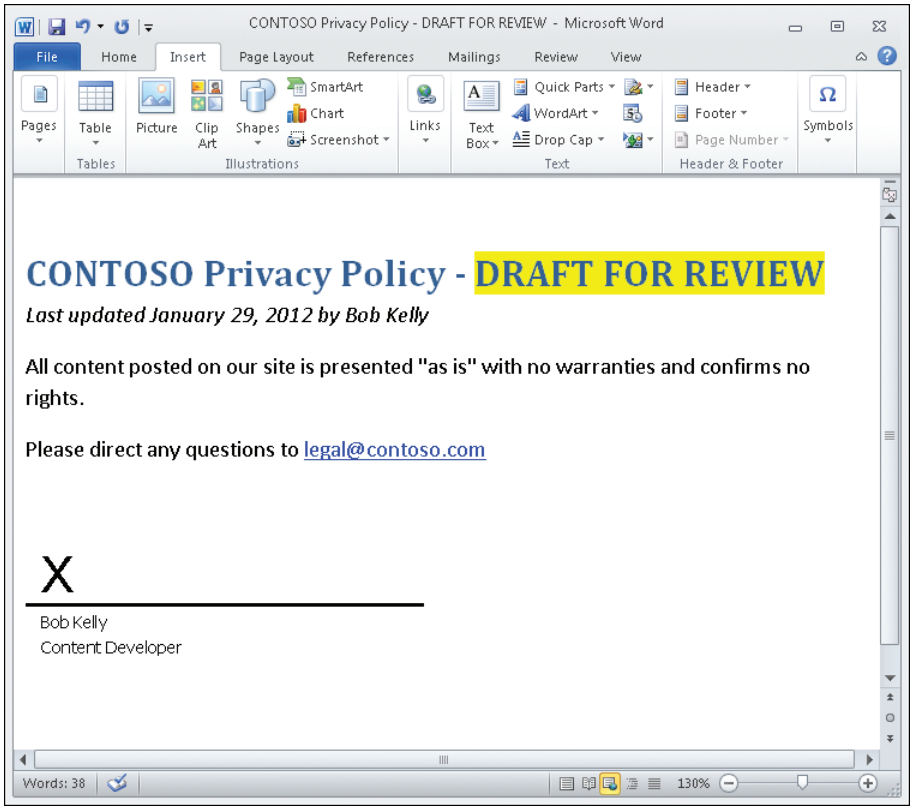
Bob is ready to sign the document he has been working on digitally so that he can send it to Alice for review. Company policy requires that every employee who handles customer-intended content must sign the content as part of the mandated review process.

Bob begins by placing his cursor at an appropriate point in the document and clicking the Signature Line item in the Text group on the Insert ribbon, where he selects Microsoft Office Signature Line:



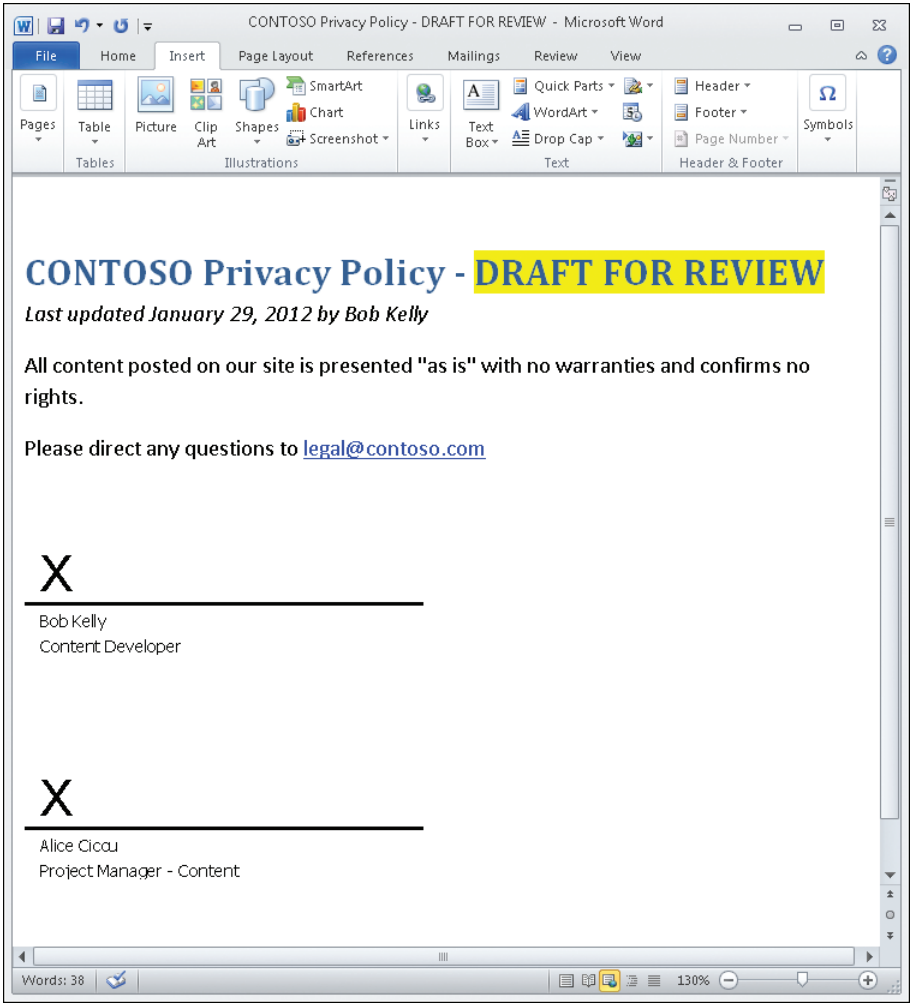
Doing this opens the Signature Setup dialog box, into which Bob then types his full name and title, email address, and some instructions for Alice, his reviewer, to follow:

Clicking OK adds a signature line graphic to the end of the document as follows:

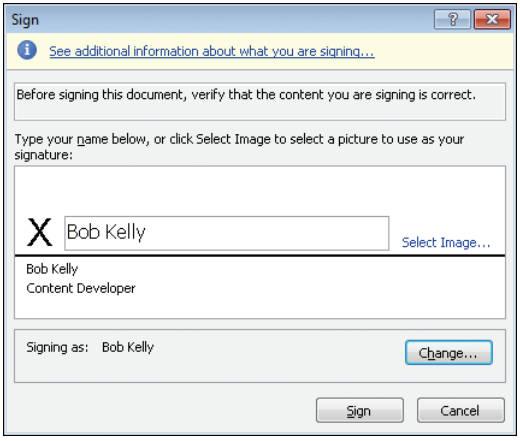


Bob now repeats the process to add a second signature line for Alice to sign the document when she reviews it. When he enters information into the Signature Setup dialog box the second time, Bob also selects the Allow The Signer To Add Comments In The Sign Dialog check box so that Alice will be able to add any comments she might have when signing off on the document.

At this point, the document now looks like this:



Now Bob is going to add his digital signature to the document, so he double-clicks his signature line graphic to open the following Sign dialog box:



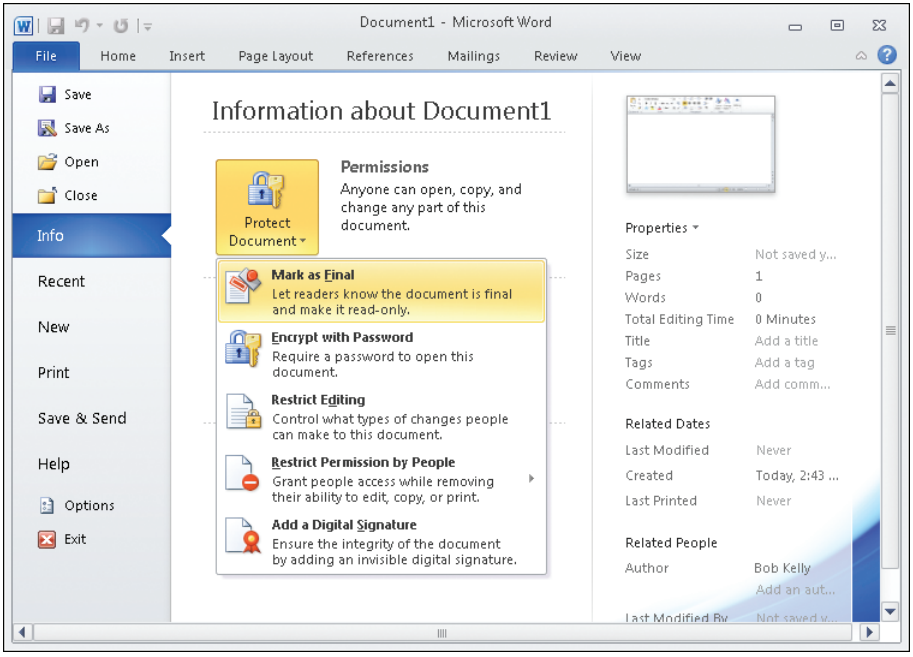
TIP

After typing his name in the field indicated by the X in the Sign dialog box, Bob clicks Sign. Doing this causes Bob's unique digital signature to be added to the document to confirm its authenticity, integrity, and non-repudiability:

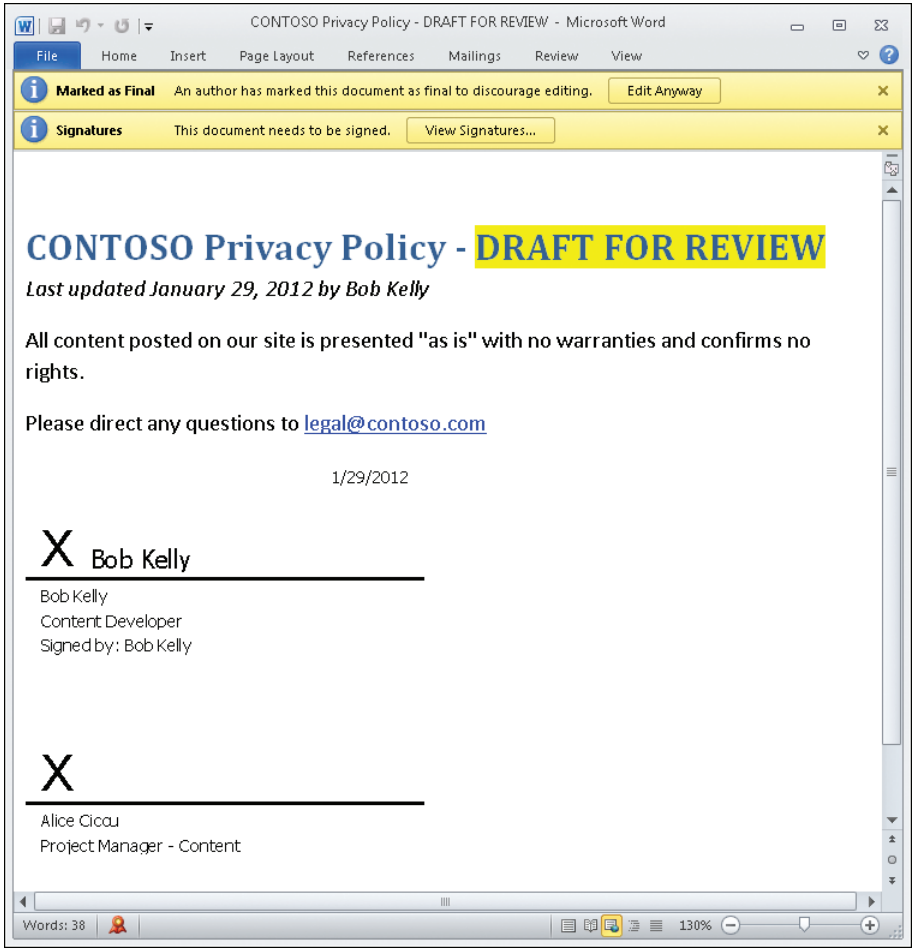
TIP

Notice the yellow message bar in the previous screenshot. Digitally signing a document in Word automatically marks the document as final, which means it's now read-only and can't be modified. Well, actually, it can still be modified if you first click the Edit Anyway button in this message bar, but doing this invalidates the digital signature that you added earlier. So, the best practice is that you shouldn't sign a document digitally until you're absolutely sure that you won't need to edit the document any further.

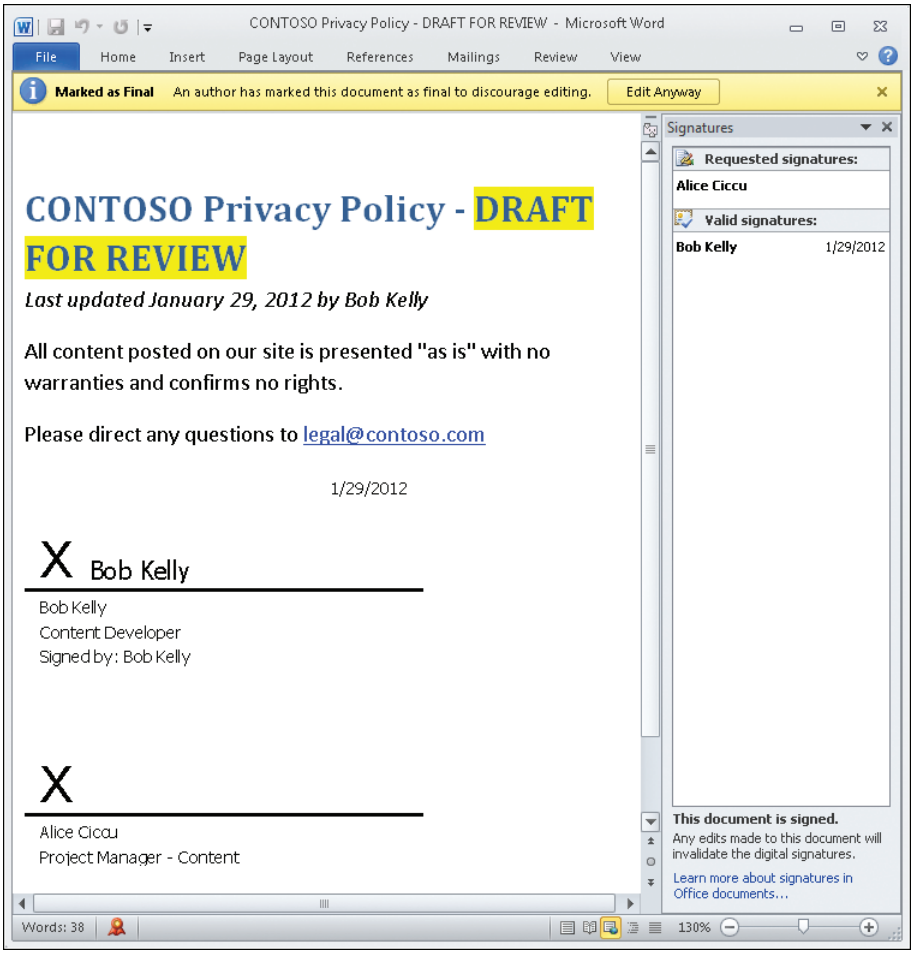
As an aside, you also can mark a document as final without signing it by selecting Backstage View, Protect Document, and Mark As Final, as follows:



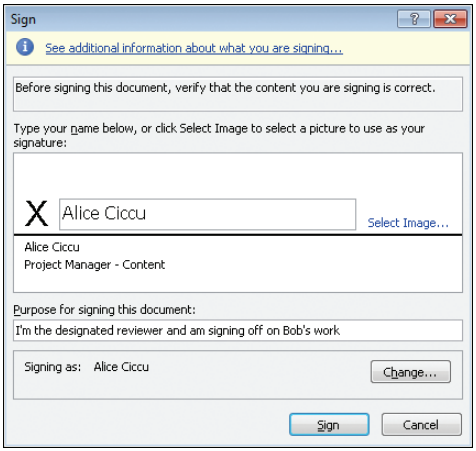
At this point, Bob is done with his work, so he sends the document to Alice for review. Alice is pretty busy working on other stuff, but she realizes that Contoso is an important customer, so she opens Bob's document to review it right away. When she opens the document, it displays two yellow message bars like this:



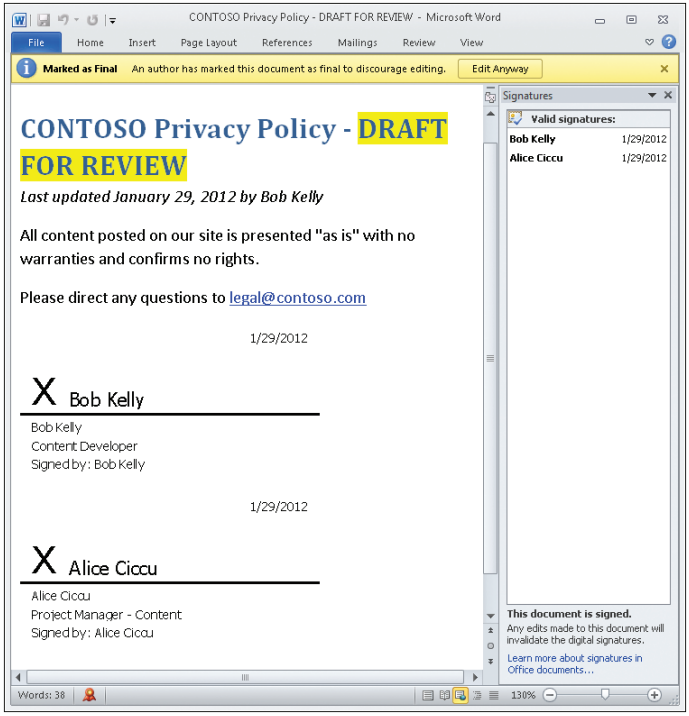
Alice clicks the View Signatures button in the second message bar. This opens the Signatures pane, which allows her to see who has signed the document with a valid signature and who still needs to sign it, as follows:



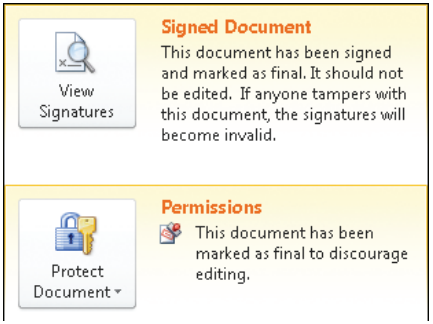
After quickly inspecting the contents of the document, Alice decides that it's OK, so she double-clicks her signature line graphic at the bottom of the document. In the Sign dialog box that opens, Alice types her name, as well as a comment indicating that she has the authority to sign off on Bob's work:



Alice clicks Sign, and now the document is signed by both parties and marked as final:



Backstage View also shows similar information like this:



The privacy policy is now ready to send to the customer.

TIP

BEST PRACTICES: VISIBLE VS. INVISIBLE DIGITAL SIGNATURES

You can add two kinds of digital signatures to Office documents: visible or invisible. The story in this chapter demonstrates how to add a visible digital signature (a digitally signed signature line), and you can add such visible signatures to both Word documents and Excel spreadsheets.

Invisible signatures, which also can be used in PowerPoint presentations, provide the same guarantee of authenticity, integrity, and non-repudiability, but they don't display any visible signature line in the document. Instead, all the reader normally sees is the red Signature button in the status bar at the bottom of the document:

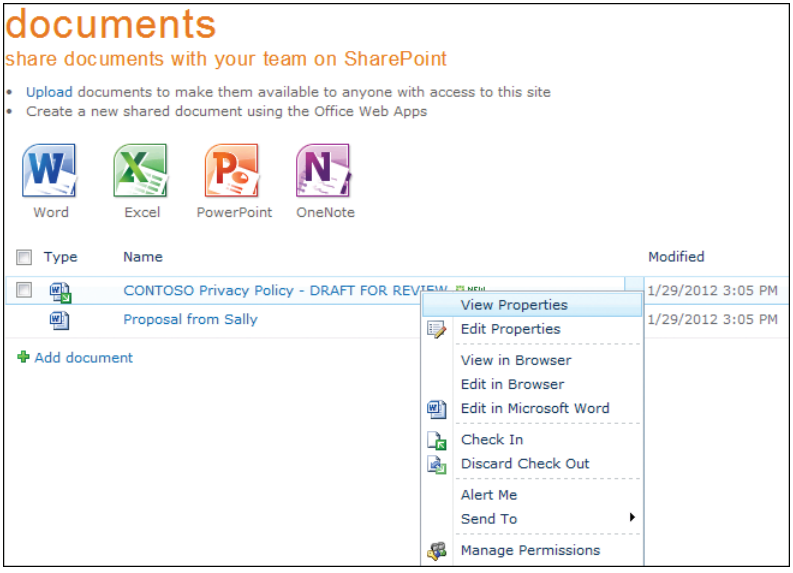
When might you use a visible signature in a document, and when would an invisible signature be better to use? Visible signatures can be helpful to organizations that need to reduce the risk involved with such electronic transactions as signing contracts or agreements because they provide a visible record of what was signed and can be verified in the future if needed. Visible signatures also can be useful when working in teams where each individual involved in a process needs to sign off on their work on the document.

Invisible signatures, on the other hand, are generally added simply to assure the authenticity, integrity, and origin of a document. For example, a business that produces software and accompanying documentation might add its invisible digital signature to both the software code itself and to the documentation to guarantee to customers that neither has been tampered during distribution.

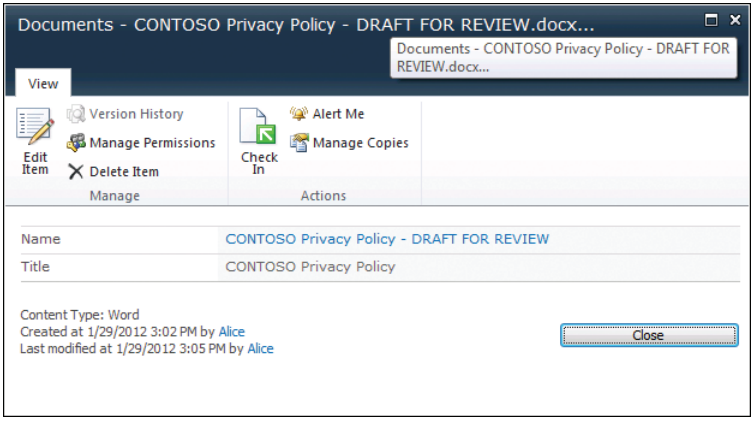
To add an invisible signature to a Word document, switch the focus to Backstage View and click Info. Then, in the Permissions section, click Protect Document, select Add A Digital Signature, and follow the prompts.

What About Office 365?

What if your organization has purchased a subscription for Office 365? Can you view or modify document properties, clean up documents, and sign them using Word Web App? At present, the Office Web Apps are missing some of the functionality in the full Office 2010 suite. For example, if Bob uploads the Word document that he is working on to his organization's SharePoint Online team site, he can view or edit the document's properties from the team site like this:

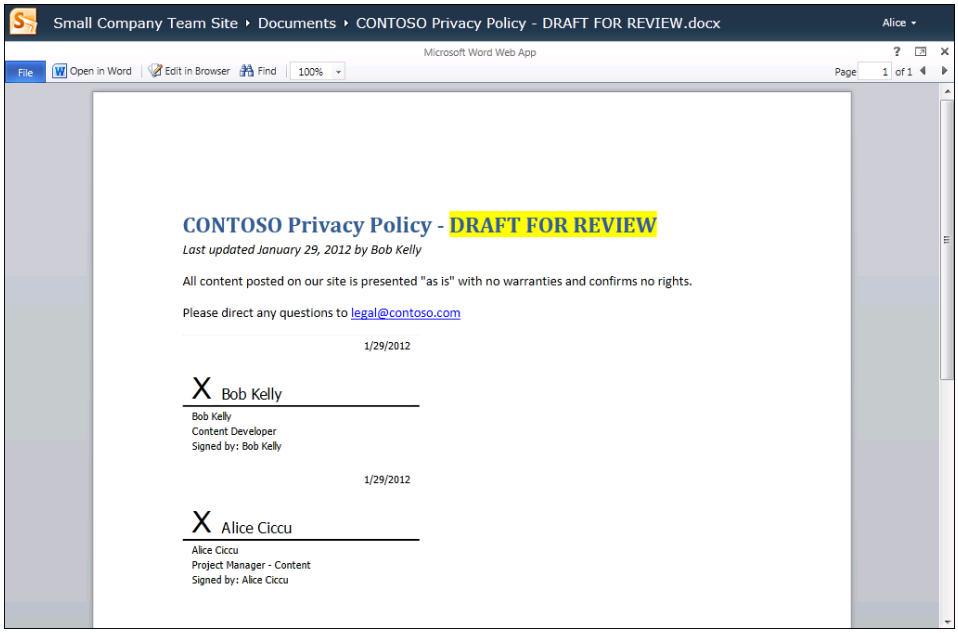


But he can only view (or edit) the name and title of the document:

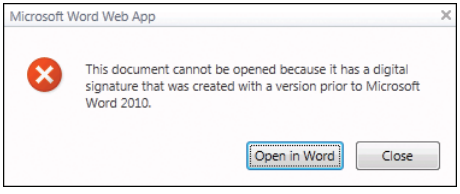


Unfortunately, none of the other document properties are accessible when using Word Web App. And there is no Document Inspector functionality in the Office Web Apps, so Bob can't use Word Web App to clean up his document prior to sharing it with the customer.

What about digital signature functionality in the Office Web Apps? When Bob selects View In Browser to display his digitally signed document using Word Web App, he sees the visible signature lines in the document:



But when he clicks the Edit In Browser button on the Word Web App toolbar, he gets the following message:



This is actually misleading, because Bob did in fact use Word 2010 to create and sign his document, but at least it shows that the Office Web Apps do not yet support digitally signing documents or editing signed documents. They may in the future, of course, if Microsoft decides to add more Office 2010 functionality to the Office Web Apps.

Of course, many businesses that purchase Office 365 subscriptions also may purchase Office 2010 Professional licenses with the subscriptions, so users can download and install the full Office 2010 programs to use their additional functionality when needed. But at this time, the Office Web Apps are more limited in what they can be used for in terms of their security and privacy capabilities.

Summary

Office documents can contain hidden information that is not normally seen when viewing a document using a functionality called document properties.

Document properties often contain sensitive or proprietary information about your company that should generally be removed from a document before sharing it with outsiders.

Document Inspector is a feature included in Word, Excel, and PowerPoint 2010, and it can be used to remove sensitive or proprietary information from documents before they are shared externally.

Digital signatures can be used to confirm the authenticity, integrity, and non-repudiability of Word, Excel, and PowerPoint documents.

Digital signatures come in two forms, visible and invisible, and each type has its specific use.

CHAPTER 4

Carol Collaborates on Some Content

IN THIS CHAPTER, YOU WILL

- Learn how to encrypt a Microsoft Office document with a password.
- Learn why passwords that are used to encrypt Office documents may have to meet length and complexity requirements in certain environments.
- Learn how to restrict the editing of a document so that only certain people can edit it, and only in certain ways.

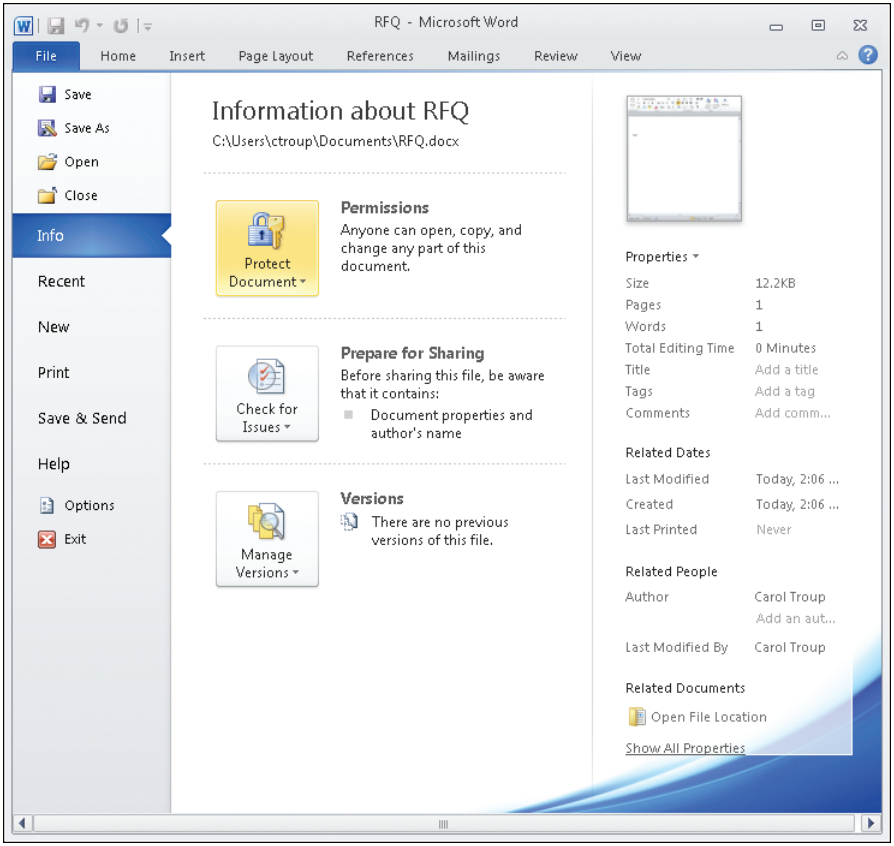
CAROL WORKS with Bob in Alice's department in the head office of Northwind Traders. They've just finished working on a request for quote (RFQ) document for one customer, and it's now ready to send to the customer for consideration. Because of the consequences of some occurrences of misdirected documents in the past, Carol wants to ensure that if the RFQ falls into the wrong hands, the information in it won't be accessible. Therefore she decides to encrypt the document with a password. She then privately phones the customer to tell her the RFQ is in transit to her, verbally provides her with the password for unlocking the document, and asks her not to share the password with anyone outside her organization.

After doing this, Carol returns to a research document in Microsoft Word that she has been working on and decides to send it to Bob for him to work on. She wants Bob to review the entire document and provide feedback by inserting comments as appropriate. She doesn't want Bob making any modifications to the document except for one section, which she wants him to be able to edit if he thinks it may be necessary. Once Bob has done this, he is to return the document to Carol for her to finish it.

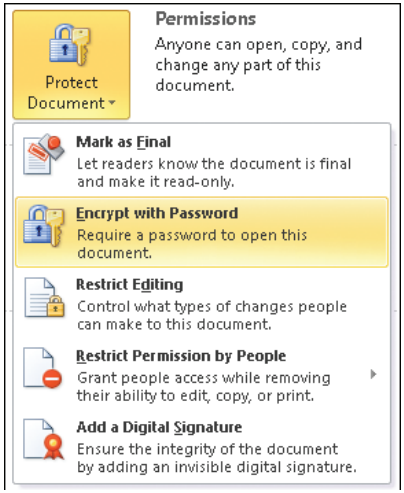
Encrypting a Document

The RFQ that Carol and Bob have been working on is ready to send to the customer, so Carol decides to encrypt the document with a password. *Encryption* is the process of converting understandable information (plaintext) into something that seems to be random and meaningless (ciphertext). A document that has been encrypted is almost impossible to decode without knowing the *secret key* used to encrypt it. Encryption is generally used to ensure the confidentiality of documents, messages, and other forms of transmitted information. You can encrypt a Word document by specifying a password. Word then generates a secret key from this password and uses it to make the document unreadable to all except those who know the password.

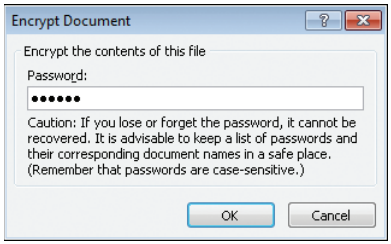
To encrypt the RFQ document, Carol selects the Info option in Backstage View and uses the Permissions control as follows:



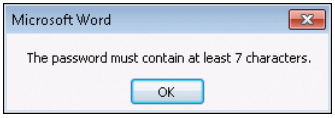
Clicking Permissions allows her to select the Encrypt With Password option from the various options displayed:



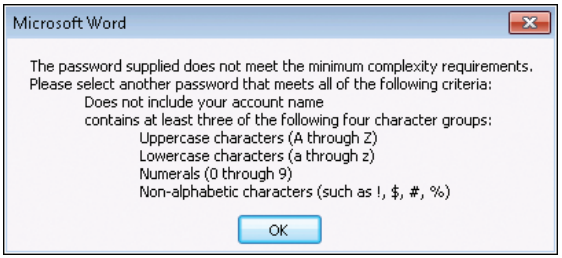
Selecting the Encrypt With Password option displays an Encrypt Document dialog box, and Carol types a six-character password where indicated:



When Carol clicks OK in this dialog box, she is surprised that Word says the password is too short:



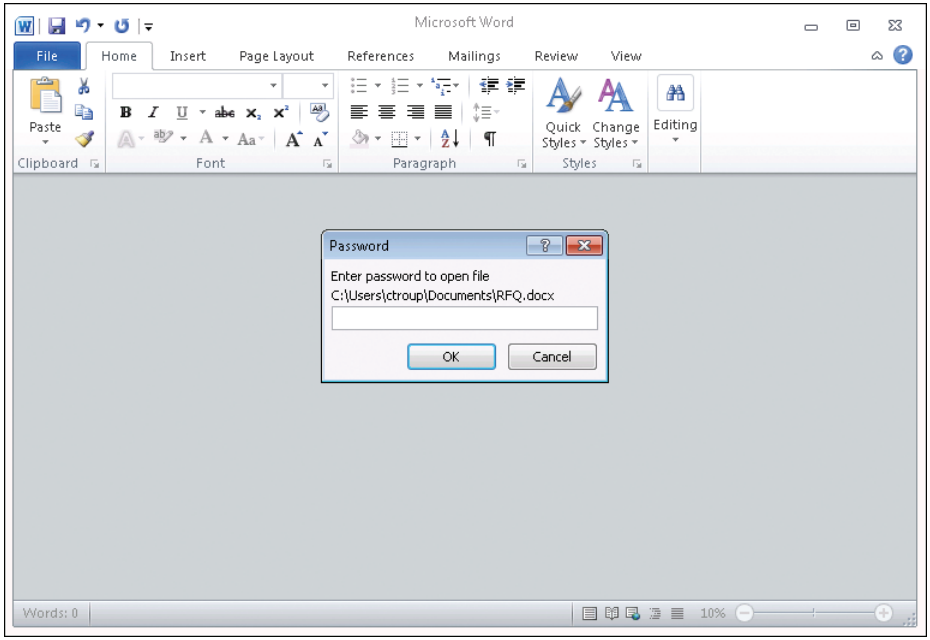
After clicking OK to close this message, Carol tries typing an eight-character password in the Encrypt Document dialog box. Unfortunately, when she clicks OK this time, she sees a message indicating that the password she supplied is insufficiently complex:



What's happening here is that the administrator of Northwind Traders has configured the Office 2010 password policies for the network so that users of Office programs have to specify passwords that meet certain length and complexity requirements when they want to password-protect their documents. In previous versions of Office, users could specify any password they wanted when encrypting documents. As a result, users often used short and simple passwords when encrypting sensitive business information. But with Office programs, long and complex passwords generate strong keys that result in strong encryption; on the other hand, short and simple passwords generate weak keys that result in weak encryption.

Because users might try to ignore a company's written security policy that says "Users must use complex passwords of at least seven characters when password-protecting Office documents," it would help if IT had a way to implement a technical control that would force users to specify such encryption passwords. Office 2010 supplies this capability by enabling IT to use Group Policy to enforce this requirement for targeted users in an organization. So Carol must be one of those targeted users.

Now that Carol understands the situation, she supplies a password of the required length and complexity to protect the RFQ, and then she saves the document and sends it to the customer. When the customer receives the RFQ and attempts to open it in Word, she is prompted to supply the password needed to decrypt the document from ciphertext back into readable plaintext, as follows:



If she doesn't know the password, she won't be able to open the document for viewing or editing.

■ **Five-Minute Exercise** **Check with your help desk and find out if the IT department is enforcing password length and complexity requirements for Office 2010 users in your organization.**

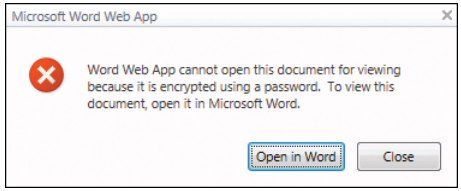
BEST PRACTICES FOR CHOOSING PASSWORDS

If your IT department isn't enforcing password policies for Office 2010 users, you should still be careful how you choose a password when protecting a document. The best practice is to always use a *strong password*, which should be eight or more characters in length and include letters, punctuation, symbols, and numbers. In addition, be sure to use all the keys available on the entire keyboard to construct your password, not just the letters and characters you use or see most often. In general, the greater the variety of characters in your password, the stronger and more resistant to password hacking it is. Other good password practices include to change your passwords frequently and to avoid using the same password for everything you need to access. For example, don't use the same password you use to purchase things online as you do to access your bank account online.

One good way of creating long, complex passwords is to begin with a sentence like "Complex passwords are safer" and remove the spaces between the words, which gives "Complexpasswordsaresafer." Next, make the password stronger by turning words into shorthand or intentionally misspelling a word (for example "ComplekspasswordsRsafer"). Finally, add some numbers that are meaningful to you after the sentence, such as "ComplekspasswordsRsafer2011."

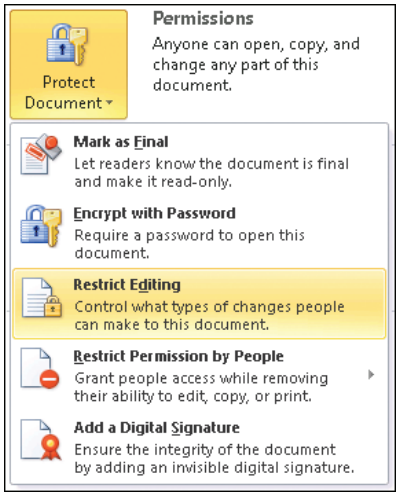
TIP

Office documents that have been password-protected can be neither viewed nor edited using the Office Web Apps. For example, if the customer tried to open Carol's RFQ in Word Web App, the following dialog box would be displayed:

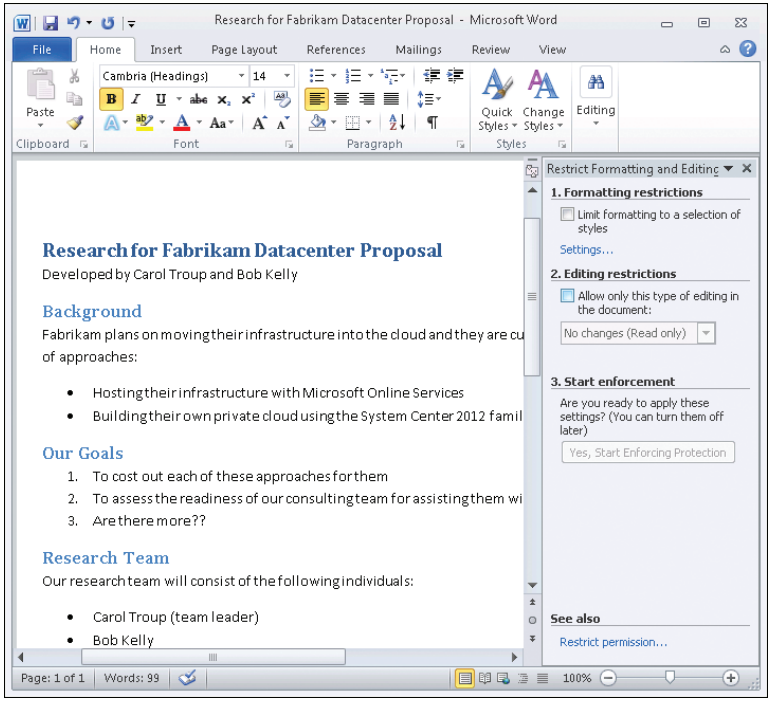


Restricting Editing

Carol begins by opening the research document in Word and switching the focus to Backstage View. With the Info option selected, Carol clicks Protect Document and selects the Restrict Editing option, as follows:



The focus automatically switches back to the Home tab, and the Restrict Formatting And Editing pane opens on the right-hand side as follows:

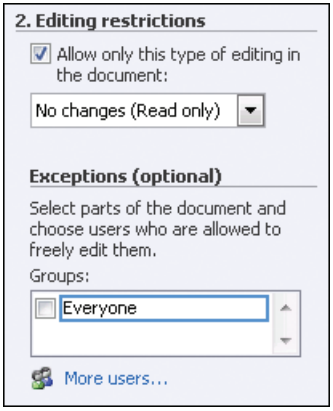


TIP

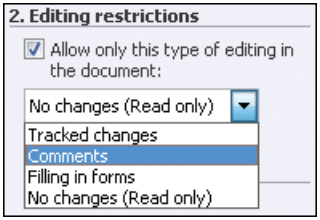
Two kinds of restrictions can be implemented in this pane:

- **Formatting Restrictions** Allow you to preserve the look and feel of a document by preventing other users from changing its styles or themes
- **Editing Restrictions** Allow you to control who can edit a document, what parts of the document can be edited, and what kinds of modifications can be made to the document

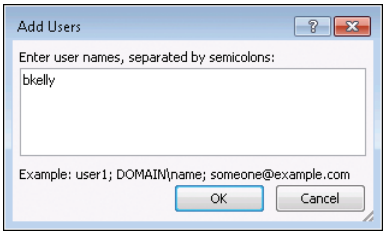
Carol's goal here is to limit the kinds of changes that Bob will be able to make to the document when he performs his review pass, so she selects the Allow Only This Type of Editing In The Document check box under Editing Restrictions:



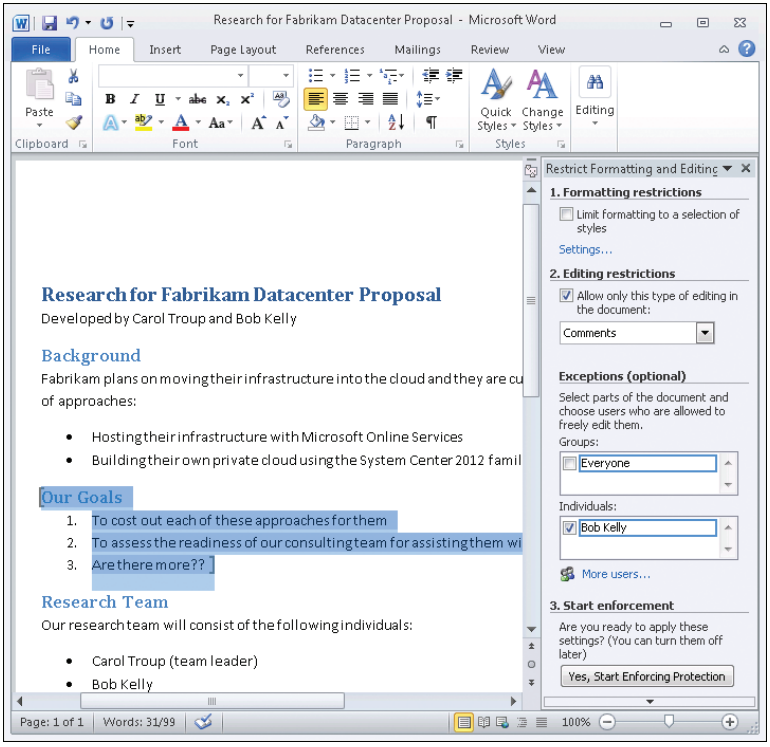
She wants Bob to only be able to add comments and not be able to make any changes to the document, so she selects Comments in the drop-down list:



To apply this restriction only to Bob, she clicks the More Users link in the Exceptions (Optional) section of the Restrict Formatting And Editing pane, as shown previously. Doing this opens the Add Users dialog box, and Carol types Bob's user name into the box:



After Carol clicks OK, the Restrict Formatting And Editing pane has an option displayed for selecting Bob by name. Carol now remembers that she also wants Bob to be able to make any changes needed to the section of the document titled "Our Goals," so she uses her mouse to select and highlight this portion of the document and then puts a check box beside Bob's name, as shown here:



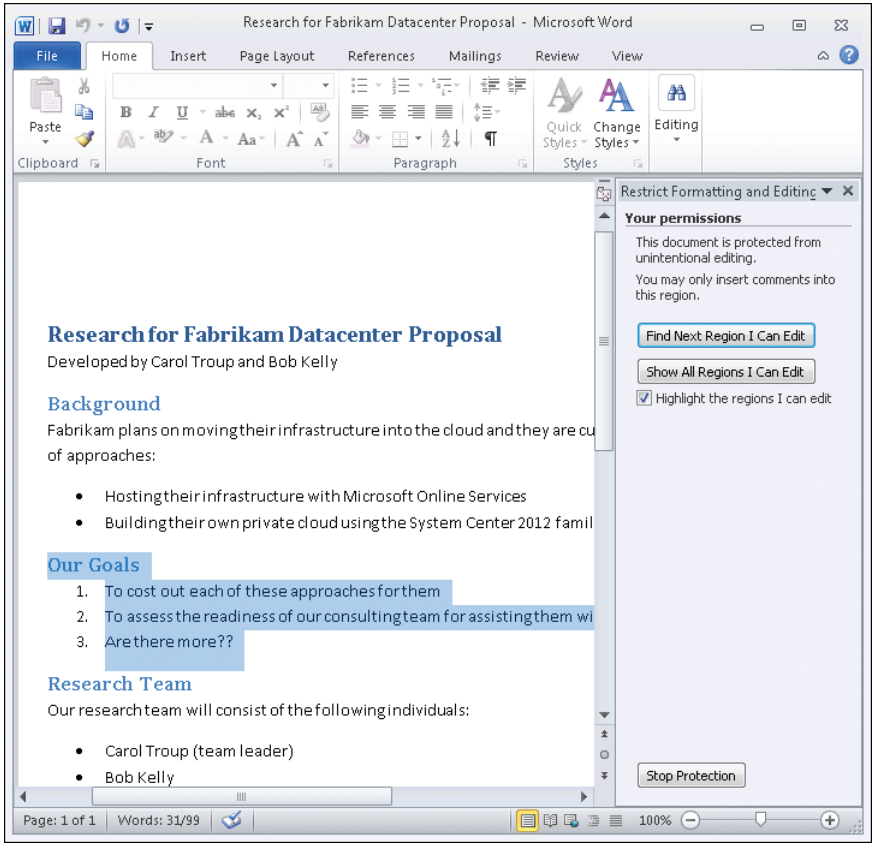
There should be two results of Carol performing all these steps:

- Bob should be able to insert comments anywhere in the document.
- Bob should be able to edit the portion of the document enclosed with square brackets, but not be able to edit any other portions of the document.

Satisfied with her selections, Carol clicks Yes, Start Enforcing Protection. The following dialog box opens, prompting her to choose a method for enforcing the selected protection settings:

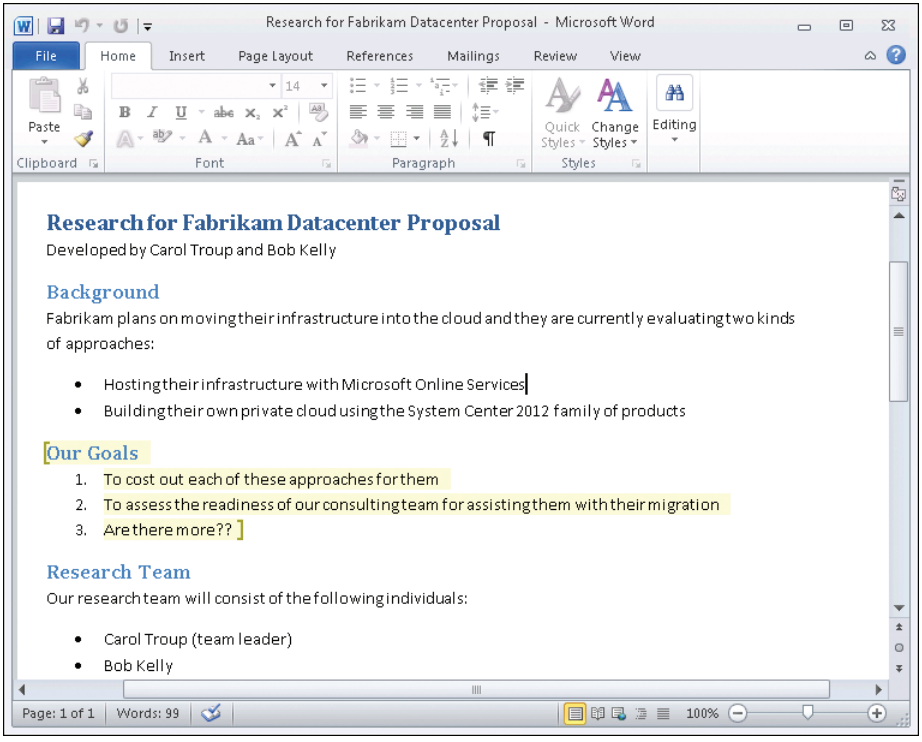
Selecting the Password option in this dialog box enables Carol to encrypt the document so that unauthenticated users won't be able to circumvent the protection settings that she has put into place for the document. Selecting the User Authentication option enables authenticated owners of the document to remove protection from it if they so choose.

Carol decides to password-protect the protection settings that she has configured for the document, so she selects Password, types the same password twice, and clicks OK. The Restrict Formatting and Editing pane changes to look like this:

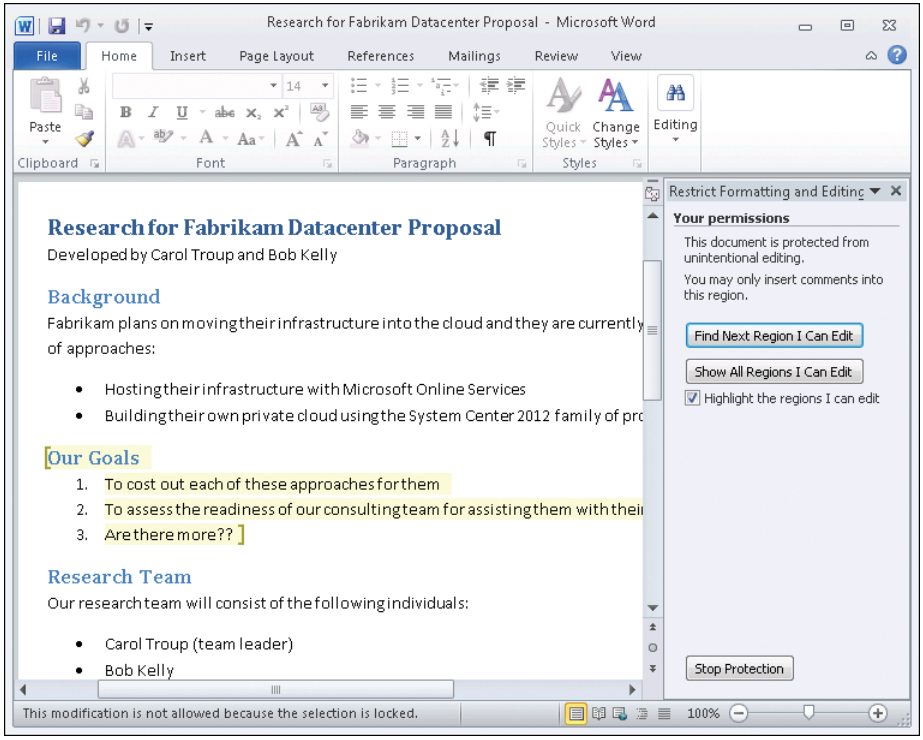


If Carol changed her mind at this point, she could click Stop Protection, and then all her previously configured protection settings would be removed from the document.

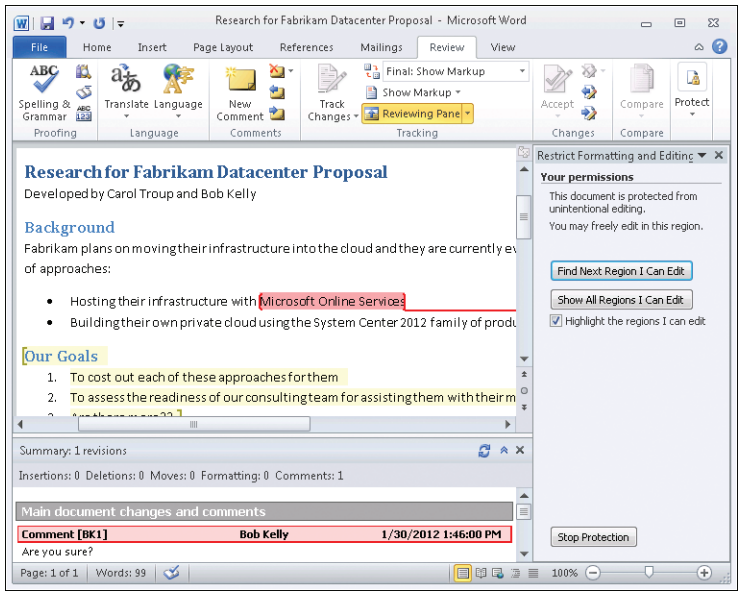
Carol now sends the document to Bob with instructions concerning what he should do with it. Bob opens the document and sees that the "Our Goals" section has been highlighted, which means that he will be able to edit that section if needed. After reading the document, however, he believes that he also should add something to the sentence about Microsoft Online Services, so he clicks in the text at the end of that sentence, as follows:



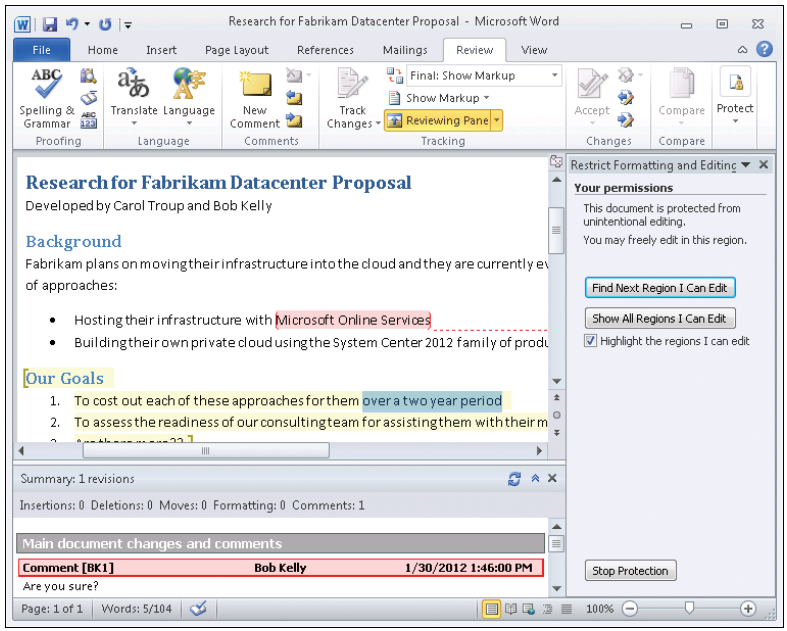
But when Bob tries to type at this point in the document, the Restrict Formatting And Editing pane opens and the message "This modification is not allowed because the selection is locked" is displayed in the status bar at the bottom of the document, as follows:



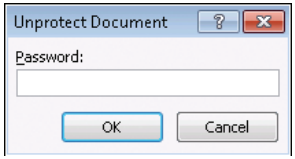
Bob now remembers Carol's instructions, so instead of trying to edit that sentence, he inserts a Word comment there instead:



He then adds a few more words to the end of the first point in the "Our Goals" section, which he is allowed to edit:

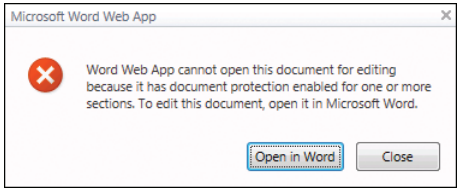


Out of curiosity, Bob wonders what might happen if he clicks Stop Protection, so he does. As a result, this dialog box opens:



Bob doesn't know the password Carol has given the document, so he closes the dialog box and finishes his work for Carol.

> Office documents that have had document protection applied using the Restrict Editing control can be viewed, but not edited, using the Office Web Apps. For example, if Bob tried to open Carol's research document for editing in Word Web App, the following dialog box would be displayed:



■ **Five-Minute Exercise** **If you have a colleague who wants to learn how to use the Restrict Editing functionality of Word, Microsoft Excel, or Microsoft PowerPoint, use this walkthrough as a starting point and explore the possibilities together.**

Summary

Office 2010 documents can be encrypted with a password to safeguard their confidentiality, and the longer and more complex the password, the stronger the encryption.

IT departments can configure technical controls that force Office users to use passwords of a given minimum length and complexity when password-protecting their documents.

You can restrict who can edit all or certain portions of your documents and what kinds of edits they can perform.

The Office Web Apps can be used to view password-protected or restricted-editing documents, but you can't make any changes to the documents using them.

APPENDIX

Learn More

IF YOU WANT TO LEARN MORE about how to use the Microsoft Office 2010 security and privacy features covered in this book, be sure to check out the selection listed here of online help articles, short videos, free online training courses, and blog posts. The links have been ordered by topic, so you can quickly find information about what you're looking for. A section at the end also covers the functionality of the Office Web Apps included with Office 365. Finally, you also can get lots of great tips by following the Office team on Twitter at *https://twitter.com/office*.

General Resources on Office 2010 Security and Privacy

Online help links:

- Microsoft Word (*http://office.microsoft.com/en-us/results.aspx?filter=1&qu=security%20and%20privacy&av=zwd*)
- Microsoft Excel (*http://office.microsoft.com/en-us/results.aspx?filter=1&qu=security%20and%20privacy&av=zxl*)
- Microsoft PowerPoint (*http://office.microsoft.com/en-us/results.aspx?filter=1&qu=security%20and%20privacy&av=zpp*)

- All Office programs (*http://office.microsoft.com/en-us/results.aspx?filter=1&qu=security%20and%20privacy&av=all*)
- Protect yourself from phishing schemes and other forms of online fraud (*http://office.microsoft.com/en-us/word-help/protect-yourself-from-phishing-schemes-and-other-forms-of-online-fraud-HA010354320.aspx*)

Short video:

- Video: What Is the Trust Center? (*http://office.microsoft.com/en-us/results.aspx?filter=4&qu=security%20and%20privacy&av=all*)

Free online training courses:

- Office 2010 Security: Protecting Your Files (*http://office.microsoft.com/en-us/word-help/office-2010-security-protecting-your-files-RZ101665538.aspx*)

Blogs:

- Word Blog (*http://blogs.office.com/b/microsoft-word/*)
- Excel Blog (*http://blogs.office.com/b/microsoft-excel/*)
- PowerPoint Blog (*http://blogs.office.com/b/microsoft-powerpoint/*)
- Office 2010 Engineering Blog (*http://blogs.technet.com/b/office2010/*)

Other:

- Microsoft Security Online Password Checker (*https://www.microsoft.com/security/pc-security/password-checker.aspx*)

Protected View

Online help articles:

- What Is Protected View? (*http://office.microsoft.com/en-us/starter-help/what-is-protected-view-HA102655267.aspx?CTT=1*)

Short videos:

- Office 2010 Security video: Security Decisions Made Easy (*http://office.microsoft.com/en-us/videos/office-2010-security-video-security-decisions-made-easy-VA101843566.aspx?CTT=1*)
- Office 2010 Security video: Protection Against Malware (*http://office.microsoft.com/en-us/videos/office-2010-security-video-protection-against-malware-VA101843474.aspx*)

- Turning off Protected View: Office 2010 Security (*http://office.microsoft.com/en-us/videos/turning-off-protected-view-office-2010-security-VA102000187.aspx?CTT=1*)

Blog post:

- Protected View in Office 2010 (*http://blogs.technet.com/b/office2010/archive/2009/08/13/protected-view-in-office-2010.aspx*)

Trusted Documents

Online help article:

- Trusted documents (*http://office.microsoft.com/en-us/word-help/trusted-documents-HA010354384.aspx*)

Short video:

- Office 2010 Security video: Why Use Trusted Documents? (*http://office.microsoft.com/en-us/videos/office-2010-security-video-why-use-trusted-documents-VA101872045.aspx?CTT=1*)

Blog post:

- Trusted Documents (*http://blogs.technet.com/b/office2010/archive/2009/09/28/trusted-documents.aspx*)

Trusted Locations

Online help article:

- Add, Remove, or Modify a Trusted Location for Your Files (*http://office.microsoft.com/en-us/word-help/add-remove-or-modify-a-trusted-location-for-your-files-HA010354311.aspx?CTT=1*)

Document Properties

Online help article:

- View or Change the Properties for an Office File (*http://office.microsoft.com/en-us/word-help/view-or-change-the-properties-for-an-office-file-HA010354245.aspx?CTT=1*)

Document Inspector

Online help articles:

- Remove Hidden Data and Personal Information by Inspecting Documents (*http://office.microsoft.com/en-us/word-help/remove-hidden-data-and-personal-information-by-inspecting-documents-HA010354329.aspx*)
- Remove Tracked Changes and Comments from a Document (*http://office.microsoft.com/en-us/word-help/remove-tracked-changes-and-comments-from-a-document-HA101822263.aspx?CTT=1*)

Digital Signatures

Online help articles:

- Digital Signatures and Certificates (*http://office.microsoft.com/en-us/word-help/digital-signatures-and-certificates-HA010354667.aspx?CTT=1*)
- Add a Signature Line (*http://office.microsoft.com/en-us/word-help/add-a-signature-line-HA102247419.aspx?CTT=1*)
- Add or Remove a Digital Signature in Office Files (*http://office.microsoft.com/en-us/word-help/add-or-remove-a-digital-signature-in-office-files-HA010354308.aspx?CTT=1*)
- How to Tell if a Digital Signature Is Trustworthy (*http://office.microsoft.com/en-us/word-help/how-to-tell-if-a-digital-signature-is-trustworthy-HA010354321.aspx?CTT=1*)
- View Digital Signature and Certificate Details (*http://office.microsoft.com/en-us/word-help/view-digital-signature-and-certificate-details-HA010370712.aspx*)
- View Additional Information and Hidden Content that Has Been Digitally Signed (*http://office.microsoft.com/en-us/word-help/view-additional-information-and-hidden-content-that-has-been-digitally-signed-HA010354325.aspx*)
- Obtain a Digital Certificate to Create a Digital Signature (*http://office.microsoft.com/en-us/word-help/obtain-a-digital-certificate-to-create-a-digital-signature-HA010354319.aspx*)

Blog post:

- Digital Signatures in Office 2010 (*http://blogs.technet.com/b/office2010/archive/2009/12/08/digital-signitures-in-office-2010.aspx*)

Encrypt with Password

Online help articles:

- Password-protect a Document (*http://office.microsoft.com/en-us/word-help/password-protect-a-document-HA010372707.aspx*)
- Password Policy (*http://office.microsoft.com/en-us/word-help/password-policy-HA010355926.aspx*)

Blog posts:

- Protect Your Document, Workbook, or Presentation with Passwords, Permission, and Other Restrictions (*http://office.microsoft.com/en-us/word-help/protect-your-document-workbook-or-presentation-with-passwords-permission-and-other-restrictions-HA010354324.aspx*)
- Enabling Password Rules for Office 2010 (*http://blogs.technet.com/b/office2010/archive/2009/10/16/enabling-password-rules-for-office-2010.aspx*)

Restrict Editing

Online help articles:

- Protect Your Document, Workbook, or Presentation with Passwords, Permission, and Other Restrictions (*http://office.microsoft.com/en-us/word-help/protect-your-document-workbook-or-presentation-with-passwords-permission-and-other-restrictions-HA010354324.aspx*)
- Restrict Changes to Files in Word and Excel (*http://office.microsoft.com/en-us/word-help/restrict-changes-to-files-in-word-and-excel-HA010354323.aspx*)
- Restrict or Permit Formatting Changes (*http://office.microsoft.com/en-us/word-help/restrict-or-permit-formatting-changes-HA010372712.aspx*)
- Allow Changes to Parts of a Protected Document (*http://office.microsoft.com/en-us/word-help/allow-changes-to-parts-of-a-protected-document-HA010372706.aspx*)
- Information Rights Management in Office 2010 (*http://office.microsoft.com/en-us/word-help/information-rights-management-in-office-2010-HA010354260.aspx?CTT=1*)

Resources on Office Web Apps and Office 365

Online help:

- Differences Between Using a Document in the Browser and in Word (*http://office.microsoft.com/en-us/web-apps-help/differences-between-using-a-document-in-the-browser-and-in-word-HA102748596.aspx*)
- Differences Between Using a Workbook in the Browser and in Excel (*http://office.microsoft.com/en-us/web-apps-help/differences-between-using-a-workbook-in-the-browser-and-in-excel-HA010369179.aspx?CTT=1*)
- Edit a Workbook that Contains Features Unsupported by Excel Web App (*http://office.microsoft.com/en-us/web-apps-help/edit-a-workbook-that-contains-features-unsupported-by-excel-web-app-HA102540964.aspx?CTT=1*)

Short videos:

- Video: What Are Office Web Apps? (*http://office.microsoft.com/en-us/videos/video-what-are-office-web-apps-VA102446424.aspx?CTT=1*)
- Video: What Is Office 365? (*http://office.microsoft.com/en-us/videos/video-what-is-office-365-VA102705845.aspx?CTT=1*)
- Office 365: A Tour for Users (*http://office.microsoft.com/en-us/videos/office-365-a-tour-for-users-HA102657904.aspx?CTT=1*)
- Get Started with Office Web Apps in Office 365 (*http://office.microsoft.com/en-us/web-apps-help/get-started-with-office-web-apps-in-office-365-HA102619009.aspx?CTT=1*)

Blogs:

- Office Web Apps Blog (*http://blogs.office.com/b/officewebapps/*)
- Office 365 Blog (*http://community.office365.com/en-us/b/microsoft_office_365_blog/default.aspx*)

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X

Z

About the Author

Mitch Tulloch was the lead author of the *Windows 7 Resource Kit* (Microsoft Press, 2009) and is a widely recognized expert on Windows administration, deployment, and security. Mitch has published hundreds of articles on a wide variety of technology sites and has written over two dozen books, including *Understanding Microsoft Virtualization Solutions: From the Desktop to the Datacenter* (Microsoft Press, 2010). He has been repeatedly awarded Most Valuable Professional (MVP) status by Microsoft for his outstanding contributions in supporting the global IT community.

Mitch runs an IT content development business in Winnipeg, Canada, that produces books, white papers, e-learning courses, and other learning materials. Before starting his own business in 1998, Mitch worked as a Microsoft Certified Trainer (MCT) for Productivity Point.

For more information about Mitch, visit his website *(http://www.mtit.com)*.

You can also follow him on Twitter at *http://twitter.com/mitchtulloch*.

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

Microsoft Press