Office 2007 Sikkerhed

Jesper Priskorn
Senior Technology Specialist
Microsoft Danmark
jpris@microsoft.com

What's A Security Model?

- Technology and user experience
- Helps customers leverage the power of Office while avoiding malicious software and attacks
- Includes but is not limited to:
  - Mitigations for extensibility: VBA, COM Add-Ins, ActiveX….
  - Presenting security choices to the user
  - Group policy and admin controls

Concerns From Office 2003

- Forces too many user decisions
- Not enough information given to the user
- Not enough fine-grained controls for admins
- Encourages users to lower security settings

Avoid Bad Security Dialogs

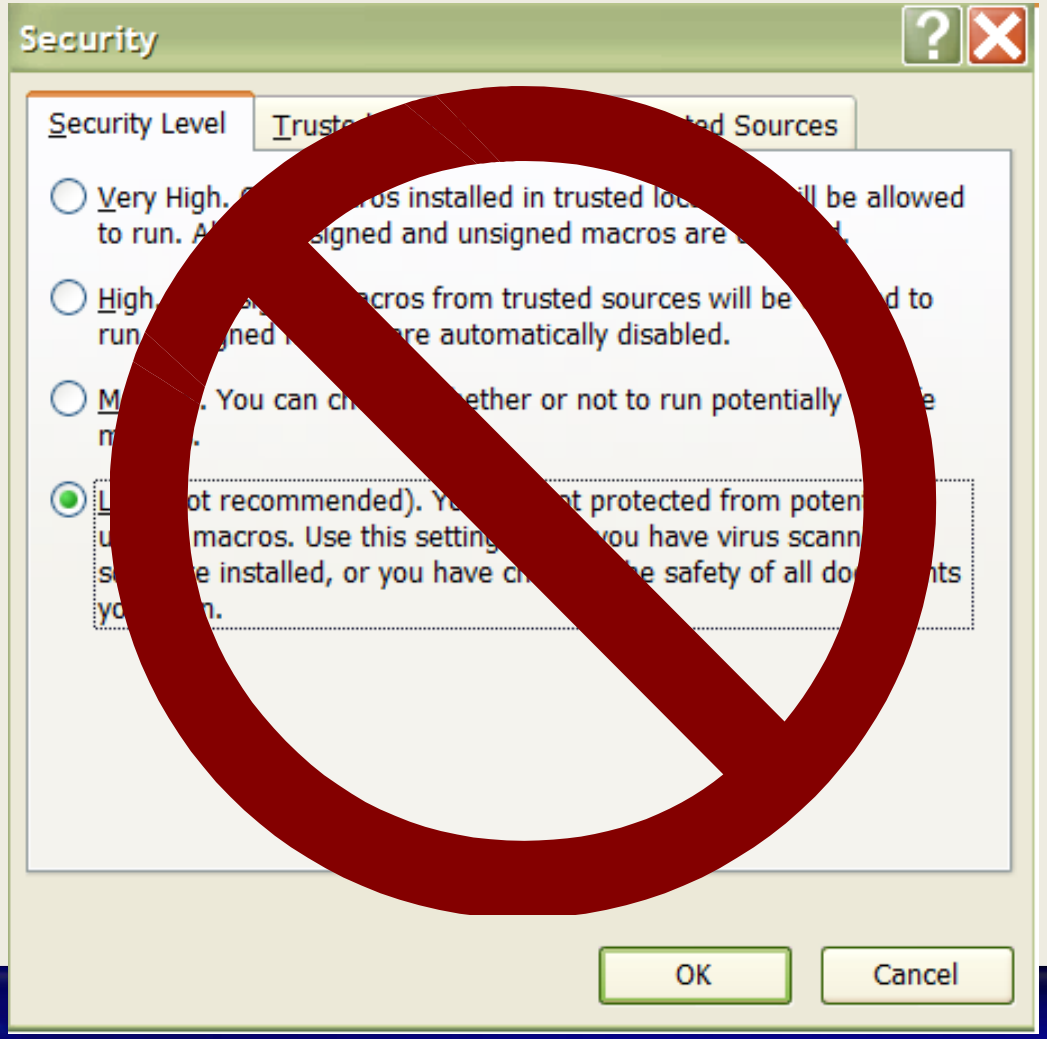
- What's the risk?
- What evidence do I have about this document?
- Can I open with the document securely?

Most users will simply open document without considering security.

Better Admin Controls

- Too many settings tied into ‘high,’ ‘medium,’ and ‘low’
- VBA settings overloaded for other purposes
- Not enough visibility into settings

No Low Settings!



Office 2007 Solutions

- Make the secure decision by default
  - Notify the user of the decision
  - Allow the user to undo the decision
- Provide new modal dialogs
  - More information, more choices
- Rework the security model
  - Make settings more discrete to scenarios
  - Provide more flexibility for admins/ISVs
- Create a new central location for settings, tools, and privacy information

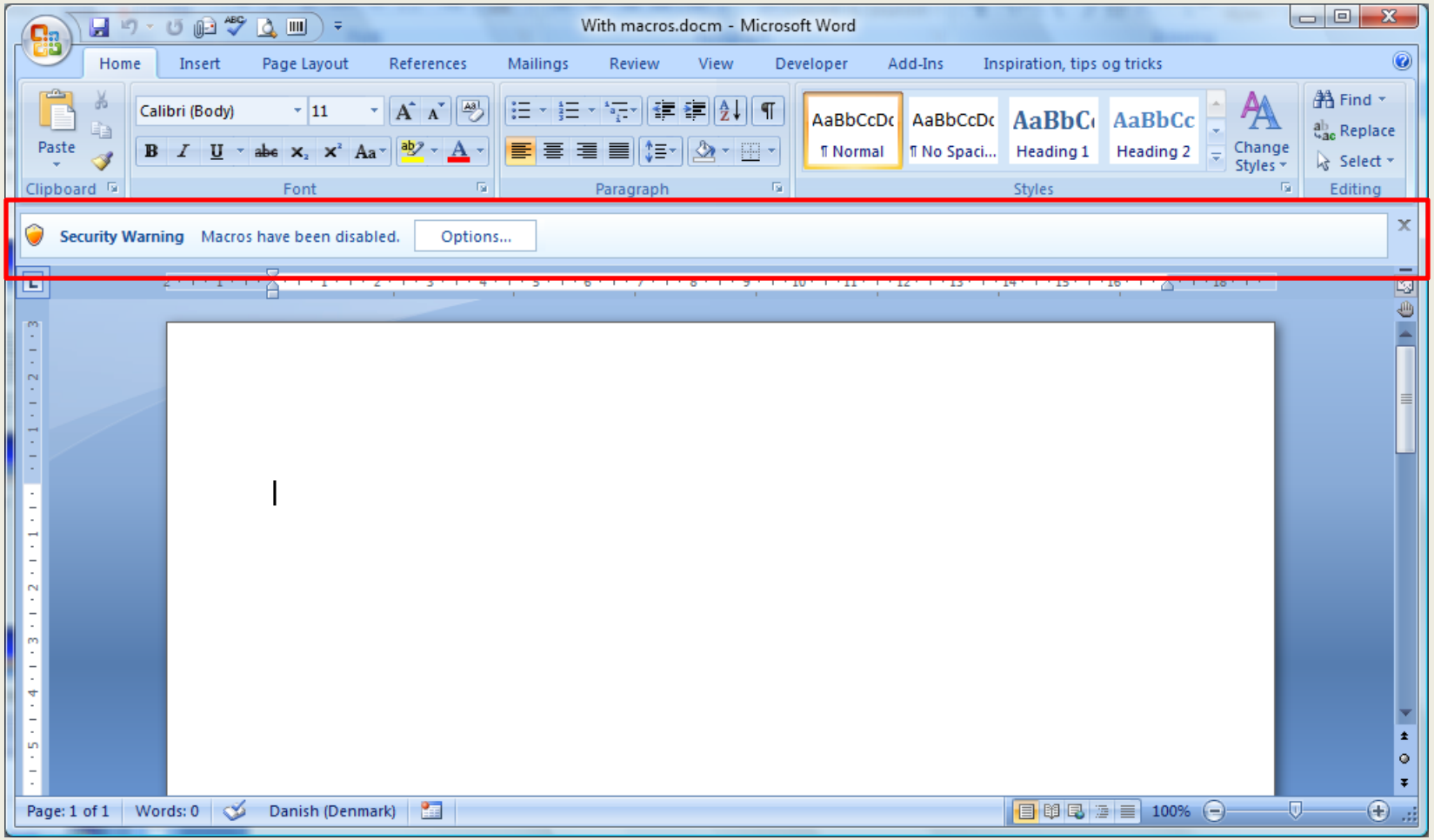
New File Format

- Includes concept of ‘macro free documents’
- Requires fewer security checks or user decisions
  - Macros & ActiveX controls just aren’t there
- Potentially better user experience in situations where macros aren’t needed

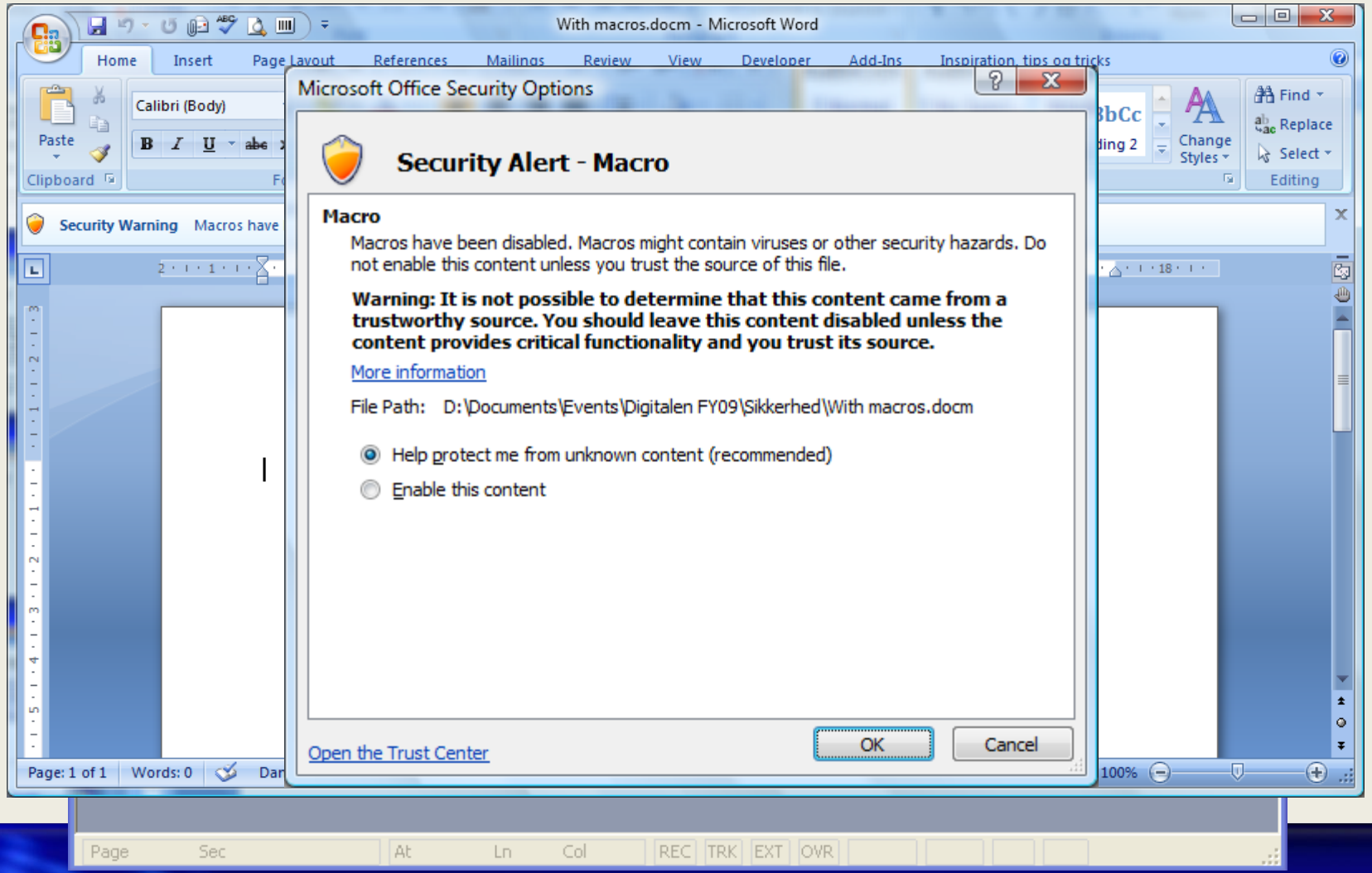
Trust Bar

- Secure by default
- Keeps user productive, can see the doc
  - Don’t start by asking them a “hard question”
- Better context to make a security decision
  - They may not actually need the macro/content
- Ability to enable content that has been disabled by default
- Secure default just “happens” and we open the doc
- Aggregate all trust decisions rather than multiple prompts

Trust Bar



Notification: Trust Bar



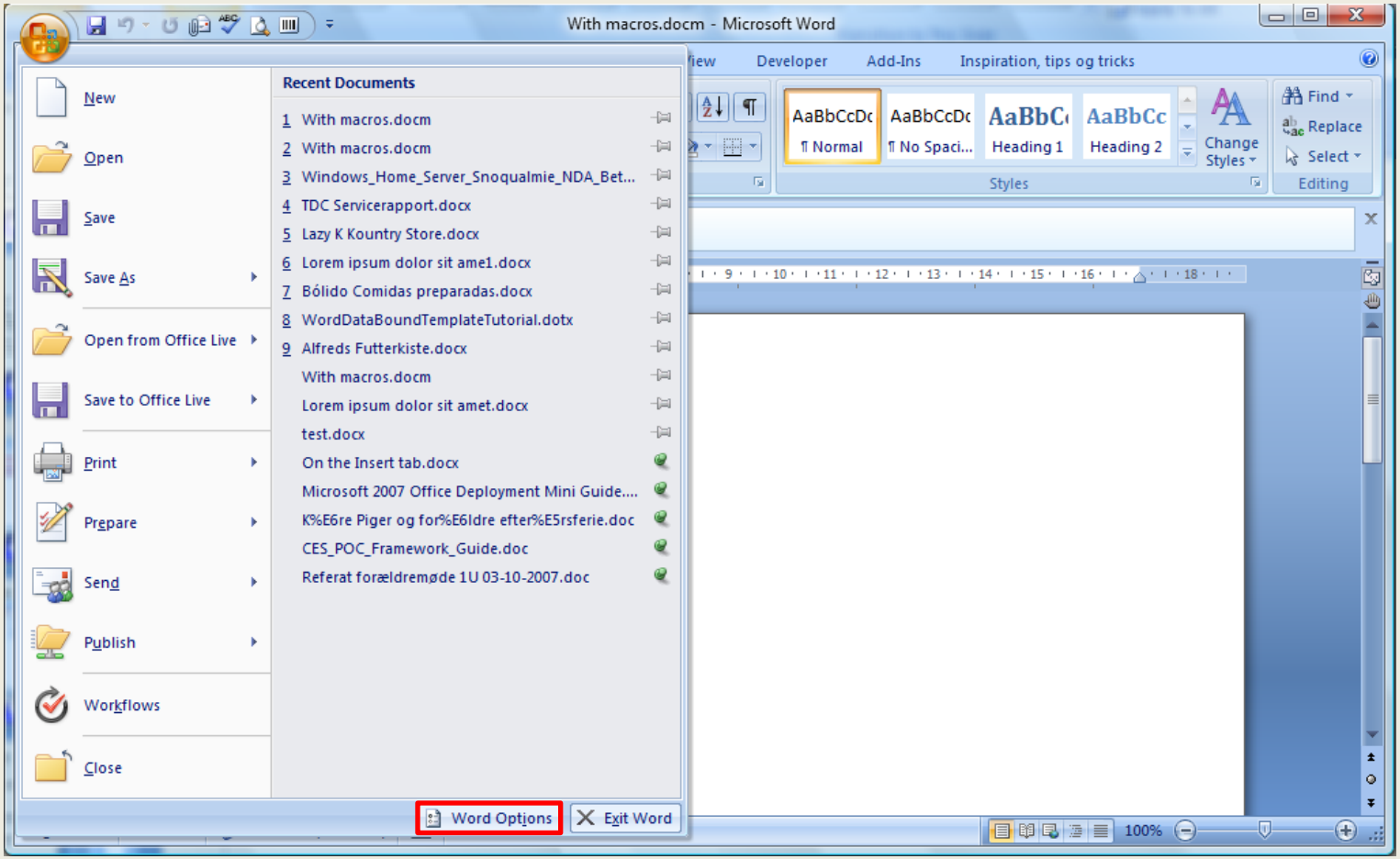
File Format and Trust Bar

DEMO

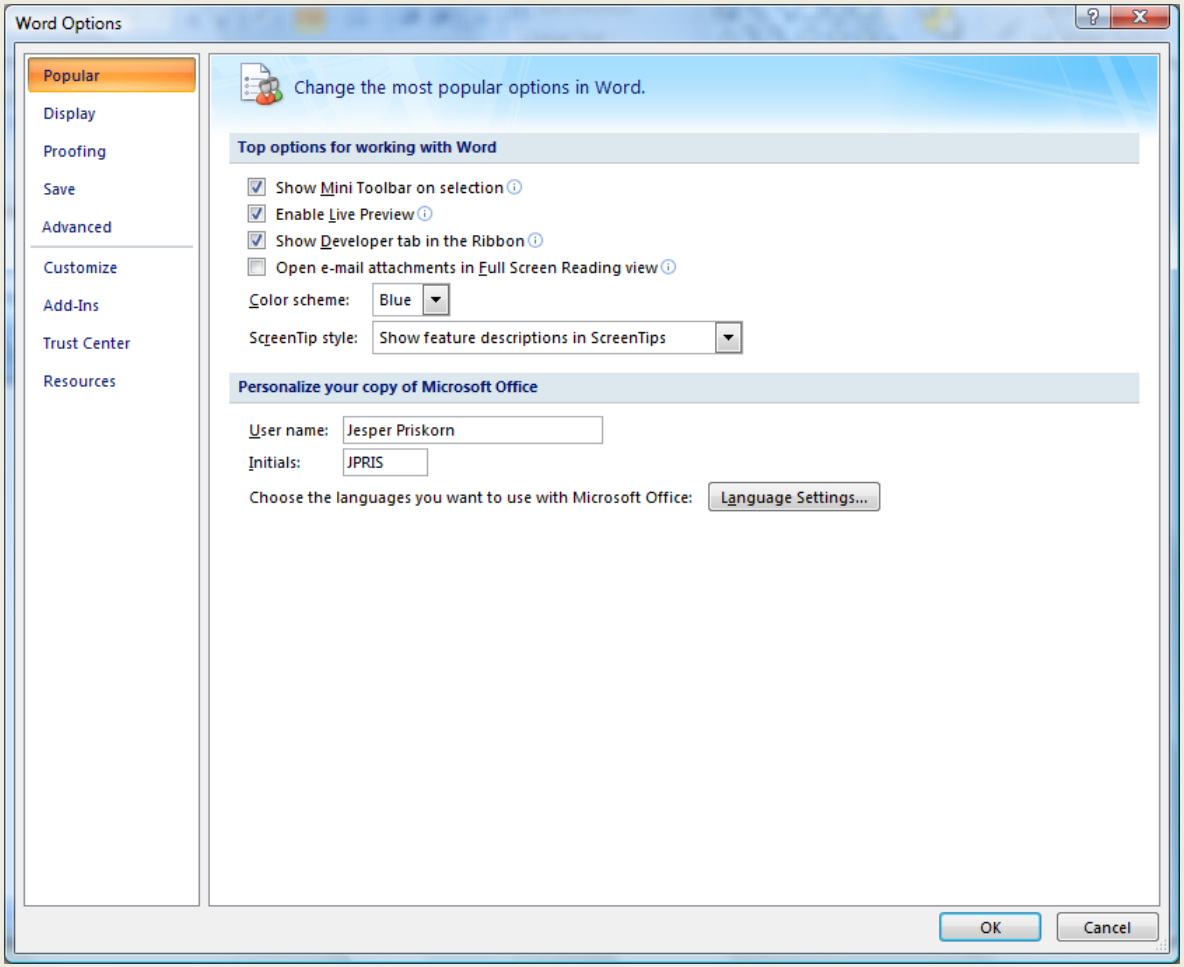
Trust Center Settings

- Component of Application Settings
- ‘Control Panel’ for security, privacy and reliability settings
- Centralizes settings from Tools.../Options/Security, Help/Service options, and Help/About, Tools/Macro/Security
- Allows users to factor settings by type

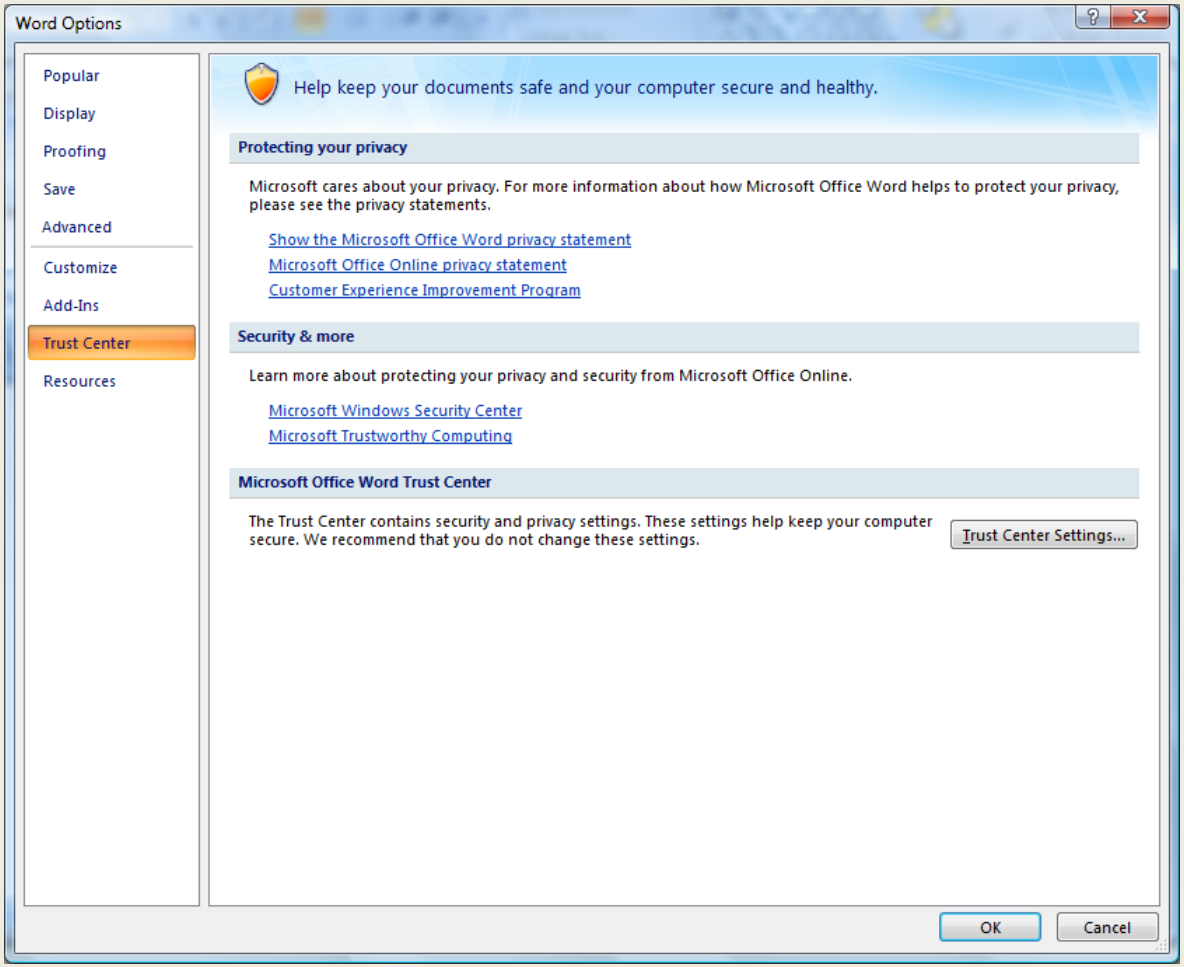
Application Settings



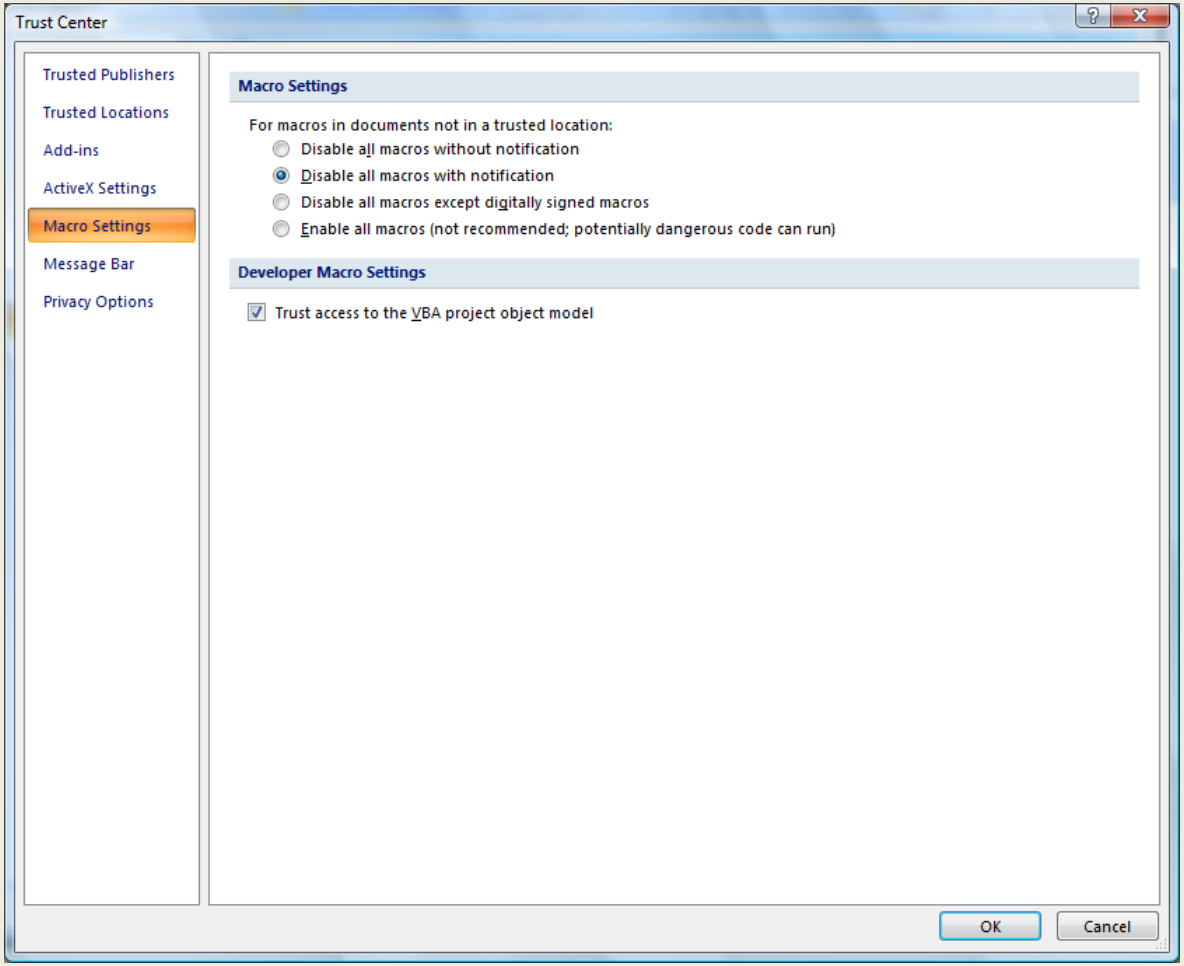
Application Settings



Trust Center Settings



Trust Center Settings



Changes To The Model

- Enhanced Trusted Locations
- Changes to VBA and ActiveX security
- New file format
- Enhanced privacy settings

Flexibility: Trusted Locations

- Trusted Locations, expanded
  - Now a Tier1 type of evidence
  - NOTE: Signatures still the preferred method
  - Access, Word, XL, PPT, Visio
- For files opened from Trusted Locations ALL content will be enabled by default
  - Macros, ActiveX settings, external links, etc.
  - Must be managed “judiciously”
- Trusted Locations
  - Added by the user from Trust Center UI or by Group Policy

Trusted Locations

- Same defaults as in the past
- Very powerful “by pass” to security settings
  - Admins can block all, publish specific set and lock
  - But need a lot of permissions to write to the users disk so threat somewhat limited
- We block some folders
  - Temp, Temporary Internet folders, “c:\”
  - Sub folders must be explicitly opted in for each location
  - Off box locations must be explicitly allowed, Internet by policy only
- Powerful option for small work groups, ad-hoc developers etc.
  - Allows you keep default secure settings for all other docs

Trust Center Settings

DEMO

VBA flags on current solutions

- Documents with “un-trusted” VBA projects will open with the project unloaded
  - Secure default (was “loaded” but disabled in the past)
- User is “in” the document, may edit it etc. before enabling any macro associated with the document
  - Current plan:
    - Word & PPT force save (if needed) and reload enabling the macros
    - XL will load and enable the macros in the “dirty” doc, firing all “file open” events
    - Not really a new state
- Automation Security (no big change)
  - Code driving the application will result in macros loading/running from documents opened by “automation”

Add-in Flags

- There is **no change in the default** add-ins security model
  - They all load enabled once installed
- But if users changes default
  - "Delay loading" Com+ Add-ins comes into play
    - In the past, if a user was prompted for an Add-in, the app "waited" for an answer
    - In Office 2007 the app will continue to load
    - User may "do work", open documents etc. before "answering" the prompt for Add-ins
    - Add-ins should be able to handle not always being loaded at boot
      - The "Com add-ins" dialog allows users do this today

ActiveX settings

- Office 2003 has reg only settings for Unsafe For Initialization ActiveX controls
  - UFI, the control is NOT safe to load with arbitrary persisted data
  - Most controls are Safe For Init (SFI)
  - Developer “choice” to declare UFI/SFI
  - Office 2003 prompts for UFI controls
- Office 2007, added UI for these options in the TC
  - Also added an option to block ALL controls

Deployment

- Custom install tool & Policy admin options
  - Both tool and template have update for new options/settings
  - Add Trusted Locations and Trusted Publishers to an Office setup
  - Deploy policy or settings to allow ONLY admin deployed locations
- As always planning is important
  - What solutions need to be deployed (ISV/internal)
  - How can these be trusted (are they signed)
  - “Special” groups, like internal developers, or “power users” who create their own macros?

Call to action

- Plan on signing solutions
  - Once singed with a cert chaining to a trusted CA the user can trust the cert and solution just runs
- Use Trusted Locations judiciously
  - The provide an alternative to signing but must be secured
  - ACLs/Permissions crucial esp on network locations
- Use the “flexibility” to target specific solutions rather than drop settings widely

Resources

- Security and protection for the 2007 Office release
  - http://technet.microsoft.com/en-us/library/cc179135.aspx
- Security and Privacy Help
  - http://office.microsoft.com/client/helpcategory.aspx?CategoryID=CH100487501033&ns=WINWORD&lcid=2057
- Outlook 2007 MAPI Reference
  - http://msdn.microsoft.com/en-us/library/cc765775.aspx