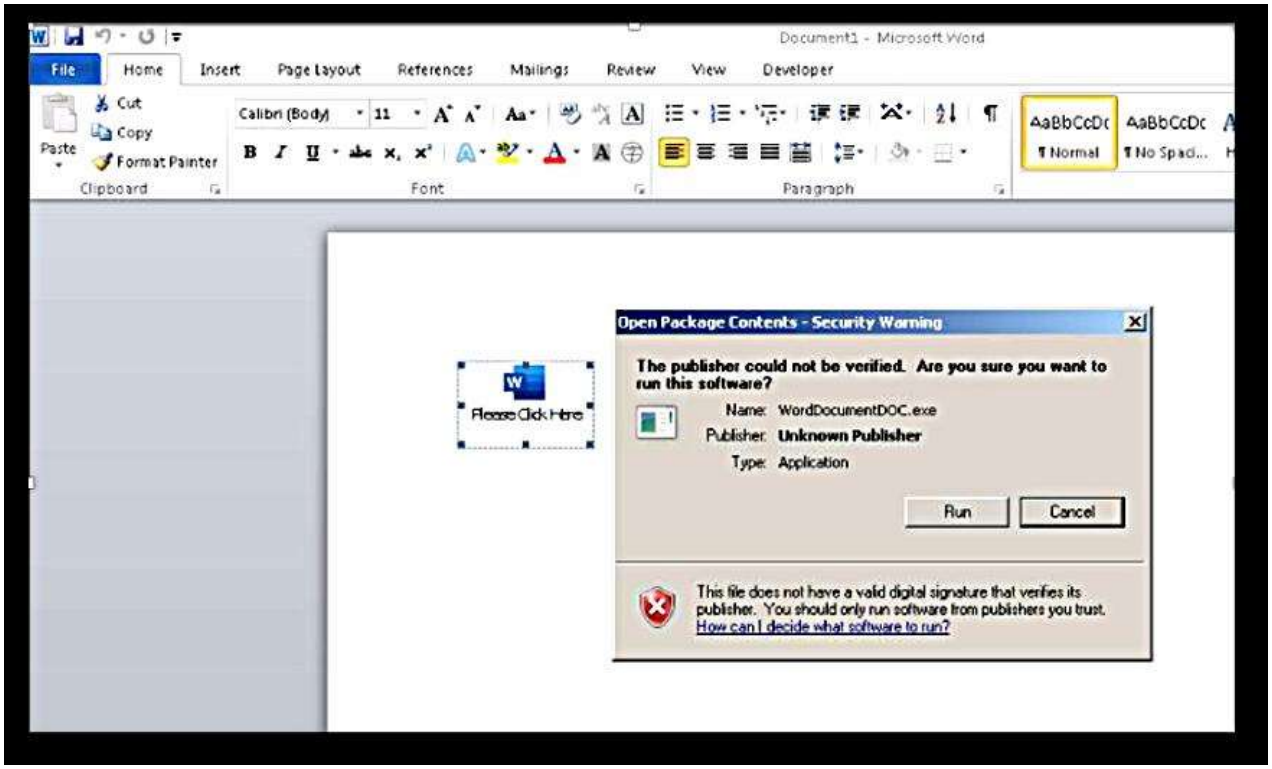
Word malware spread by rogue attachments
Who'd a thunk it? (UPDATED: July 8, 2022*; Updated[2] July 11, 2022**)

Spread the word and you'll be free
Spread the word and be like me
—The Word, Lennon/McCartney



Source: Joseph Edwards, Senior Malware Researcher at ReversingLabs
https://blog.reversinglabs.com/blog/smash-and-grab-astralocker-2-pushes-ransomware-direct-from-office-docs

Would you click Run if that button shown on your screen popped up?

If you are a regular reader of this blog, I would say the answer is No. I would not click Run.

Nevertheless, apparently in the last couple of weeks in June, scores of users around the world did exactly that, and unleashed the **AstraLocker ransomware** upon themselves and within their networks.

First revealed by ReversingLabs, as referenced above, the researchers said these cybercrooks, who they have described as employing a "**smash and grab" attack methodology** that doesn't seem to require any real coding skills; nor does this band of crooks spend much time doing any kind of reconnaissance to see if their attack victims are actually worth the effort. The central motive, according to ReversingLabs researchers, is to simply "cause disruption."

At first, I thought this news a wee bit shocking. That Microsoft Word documents can come loaded with destructive payloads has been well documented for any number of years. In fact, my own OCD behavior toward malware stems from having been a victim of the first Word Macro virus, now know as the **Word Concept Virus**. Circa 1995, the malware cost me personally $4,000 in completed work that could not be sold, with the potential for ten more similar contracts.

In an all effort to thwart these types of attacks, in April 2022, **Microsoft announced that it would now block any VBA enabled documents that orginated from the Internet**.

> **For macros in files obtained from the internet, users will no longer be able to enable content with a click of a button. A message bar will appear for users notifying them with a button to learn more. The default is more secure and is expected to keep more users safe including home users and information workers in managed organizations.**

***[ed. note] There seems to be only two constants in the IT world: constant malware and constant change. To wit: As The Hacker News reported late July 7, 2022, "Five months after announcing plans to disable Visual Basic for Applications (VBA) macros by default in the Office productivity suite, Microsoft appears to have rolled back its plans." This news derived from a blog posting by a MS employee, July 6, 2022. Nonetheless, everything herein still applies — if not more so.**

> **Angela Robertson Microsoft Jul 06 2022 08:42 AM **** Based on feedback received, a rollback has started. An update about the rollback is in progress. I apologize for any inconvenience of the rollback starting before the update about the change was made available. *****

****[ed. note^2] Well, maybe the Gnomes of Redmond just want to embarrass all of us *nattering nabobs of negativism* and other digerati. According to the most recent blog post on the topic of blocking macros by default, this is once again what Microsoft intends on doing:**

> **Update 7/8/2022: Following user feedback, we have rolled back this change temporarily while we make some additional changes to enhance usability. This is a temporary change, and we are fully committed to making the default change for all users.**

And MS explains why this change will ultimately be made. From the same blog post as above. According to Tom Gallagher, Partner Group Engineering Manager, Office Security:

> **A wide range of threat actors continue to target our customers by sending documents and luring them into enabling malicious macro code. Usually, the malicious code is part of a document that originates from the internet (email attachment, link, internet download, etc.). Once enabled, the malicious code gains access to the identity, documents, and network of the person who enabled it.**

I say read on. Learn to control macros yourself. Disable macros now and avoid the holiday rush.

Whatever may end up as the final position on enabled effort from Microsoft, VBA enabled documents are still plaguing users on the Internet. "**Researchers with Netskope said they found 776 malicious spreadsheets submitted between June 9 and June 21 that abuse Excel 4.0 (XLM) macros to download and execute Emotet's payload.**"

> **Despite the protection Microsoft released in 2022 to prevent the execution of Excel 4.0 (XLM) macros, this attack is still feasible against users who are using outdated versions of Office. It is also feasible against users who have changed the default setting to explicitly enable macros. The fact that attackers are still using Excel 4.0 Macros indicates that outdated Office versions and users who have this protection disabled are still common.**

It should be noted that **Excel 4.0 dates from 1992**.

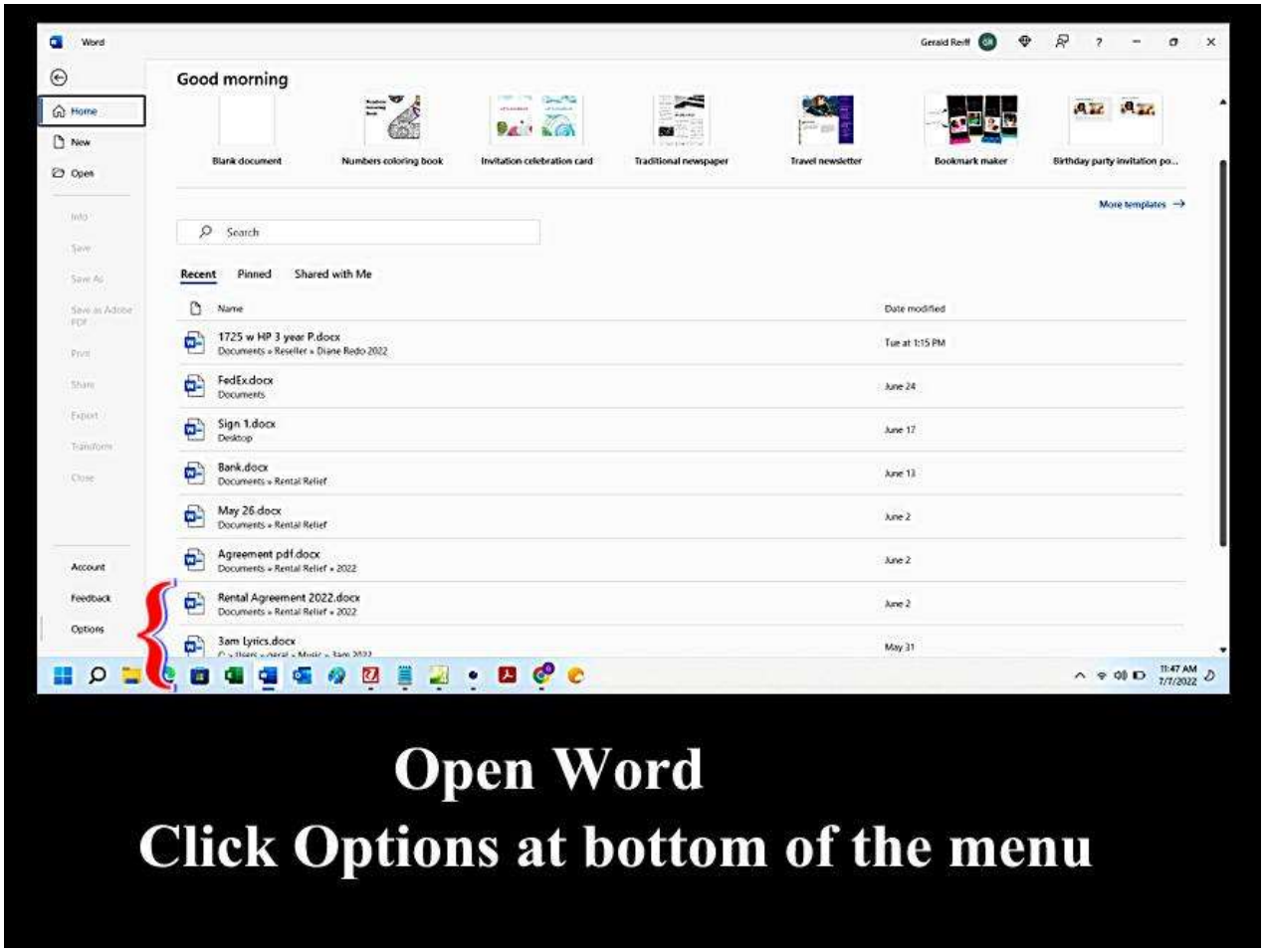
That users with half a brain would turn off macro protection in Office is unthinkable. Yet, as a threatpost.com article dates June 29, 2022, reports that one recent study showed that "**Incidents caused by unpatched systems cost organizations 54 percent more than those caused by employee error**." It is a constant theme of this blog that lazy people too fat and happy, or too hungry and miserable, to take the fifteen minutes once a month to install patches are almost as much responsible for the real damage hacking causes as do the hackers themselves. **Among server admins the failure to patch accounted for 54% of server breaches, while only 18% of breaches were the result of social engineering tricking employees into launching an attack**. It is obvious to me that more people need to read The Dispatches From the Front, or READ SOMETHING!

There is simply no reason — good or bad — to have macros enabled. So let's take a look at how we insure macros are turned off in our Office applications. To review, a macro is a small fragment of code written in the Visual Basic for Applications (VBA) programming language. It is used to automate tasks like inserting the

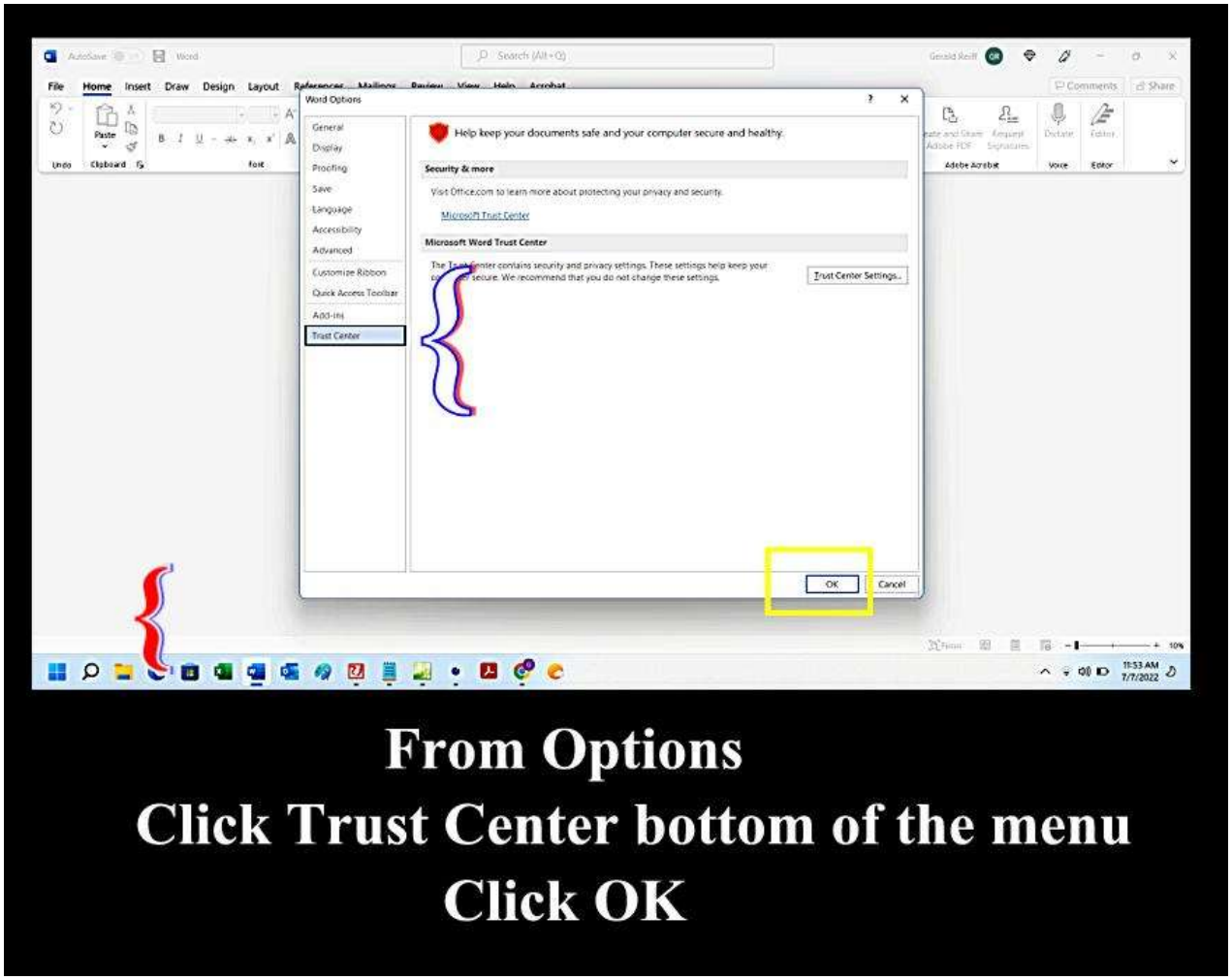
date and time into an Office document. And if you are not automating your docs or sheets, then ya'll don't need macros at all.

So here are the steps to ensure macros are turned off completely in Office. The steps are the same for each Office application, i.e. repeat for Excel, PowerPoint, etc.

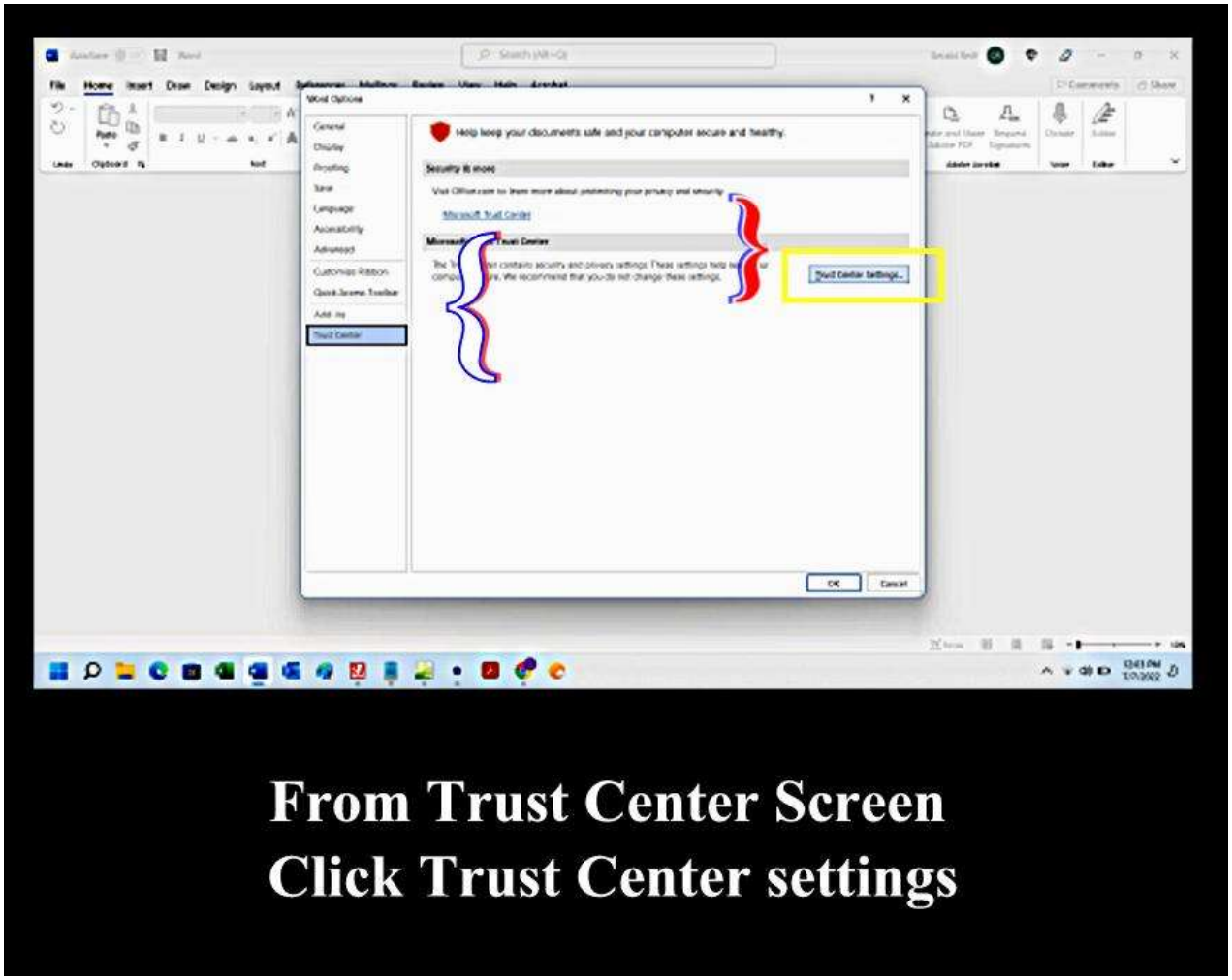
1. Open Word with no file open. Scroll down the menu to the last item labeled: "Options." Click Options



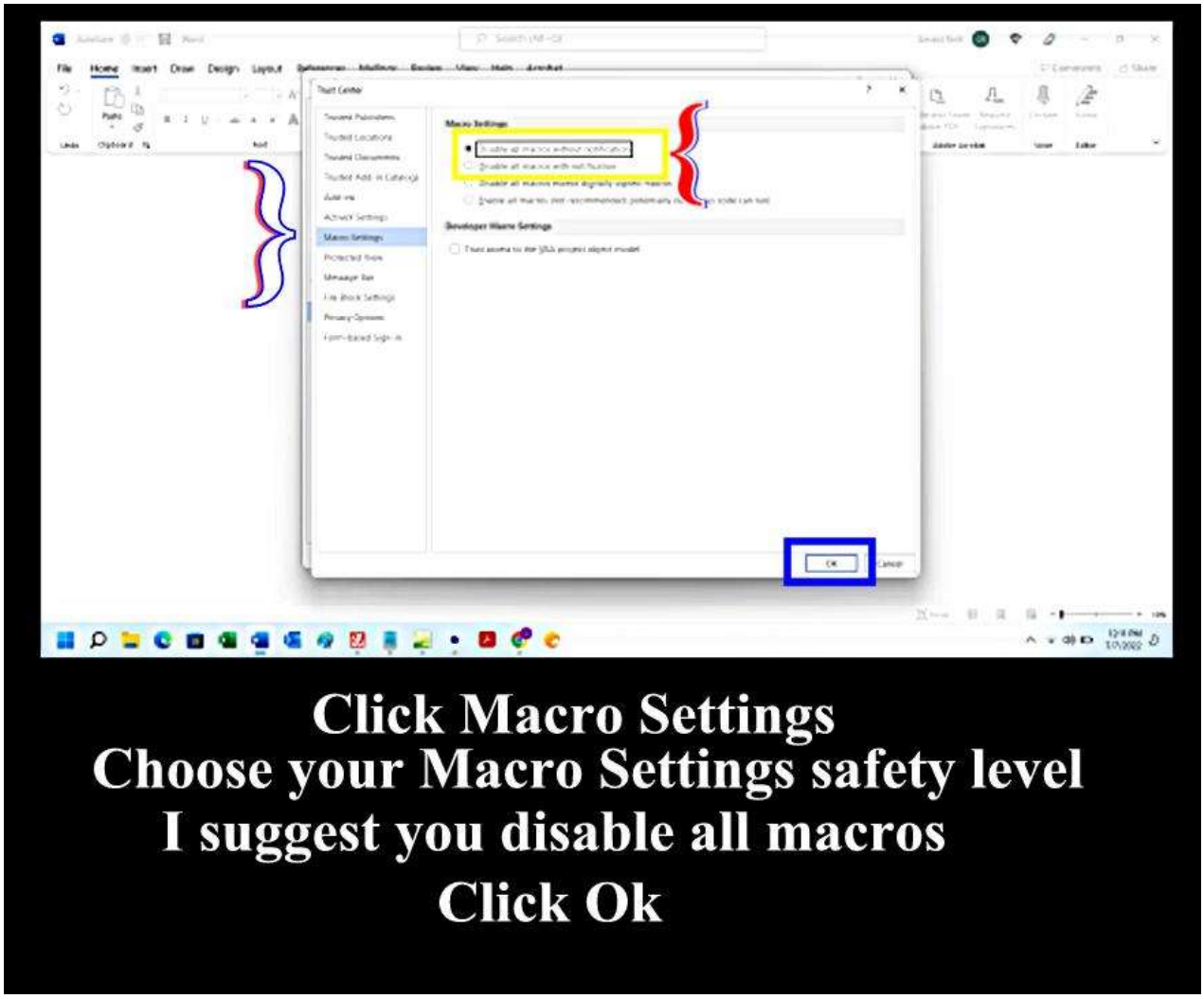
2. From the Options menu, scroll down to the bottom and click Trust Center. Click OK.



3. From the Trust Center screen, click Trust Center Settings button.



4. From Macro Settings, I suggest that you simply disable all macros and leave it at that. Click OK.



And, if you there is someone with whom you communicate, and who insists on using macros in docs you are sent, then conjure up your best Joan Rivers, and tell them to, "**Oh, Grow Up!**"

source: **https://kellybonanno.com/wp-content/uploads/2014/09/300.rivers.lr_.122210.jpg**

Ah, she was just the best, huh?

Back to Top

Gerald Reiff