Interacting with Macros Safely in Microsoft Office documents

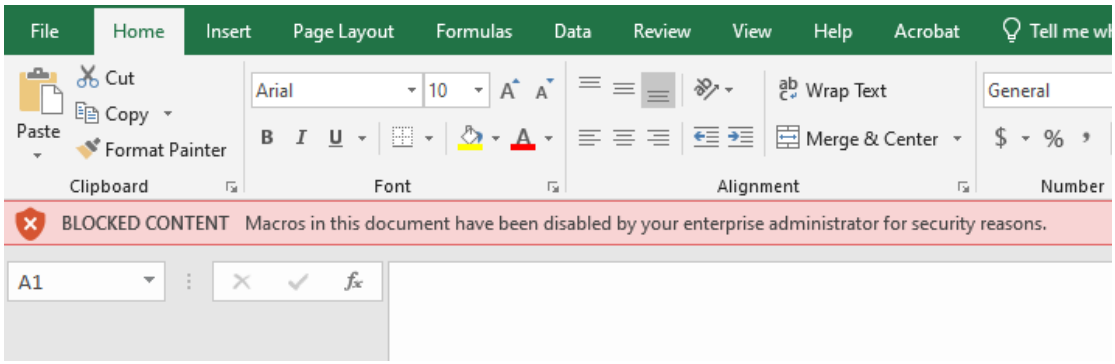
David Raco - 2025-12-01 - Comments (0) - Desktop Security

Macros are *short snippets of code* that can be embedded within **Microsoft Office files**. **Macros** were invented by **Microsoft** to support adding exciting and powerful features to **Word documents**, **Excel spreadsheets**, and other types of **Office files**, but in practice, they are often abused by bad actors to deliver malware to unsuspecting victims through **trojan Office files**.

The IT department advises extreme caution whenever you interact with macro-enabled documents! If you *don't know* or *trust* the sender of the file, you *should never* enable **macros** in an **Office file**.

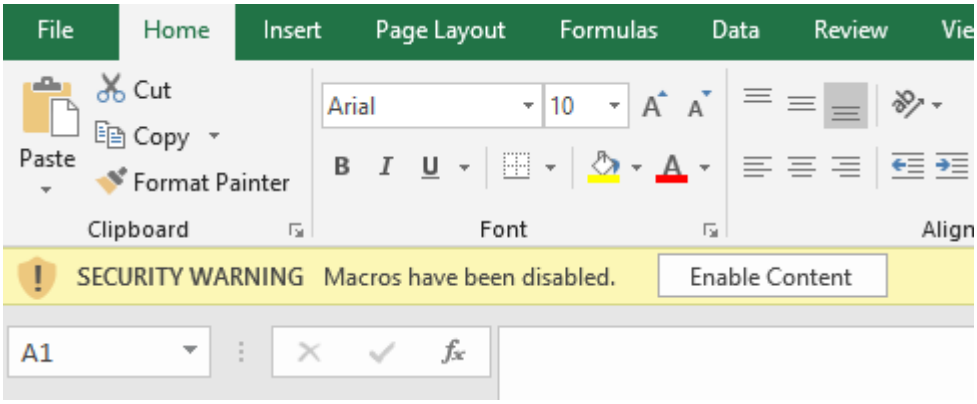
Macro Warnings

When opening an **Office file** that includes a **macro**, you may see a warning like the one below if you downloaded the file from the Internet (email, Box, etc).



If you see a warning like the one above, please forward a copy of the file to the **Information Security Manager** at infosec@sou.edu. If the file is determined to be safe and the **macros** are important, we will help you ***enable*** **macros** in the file.

When opening an **Office file** with **macros** unblocked, you will see a warning like the one below. Typically **macros** will be unblocked when the file originated from somewhere other than the Internet. You can use the **Enable Content** button to enable **macros** in the document, but be careful! If you don't know the nature of the **macros** in the file, *please* ***forward*** *a copy to* infosec@sou.edu and *await instructions* from us.



Employees can also count on their Computing Coordinators for help with these messages, and you can call our IT Helpdesk at 541-552-6900 if you need a rapid response.