Guidance Regarding Security Risk Message when Opening EmPCalc

- Microsoft has recently implemented a new security feature that is preventing essential elements of EmPCalc from functioning without some modifications to the file or to your computer.
- Contractors have reported being impacted by these changes with a Security Risk error when opening EmPCalc after downloading from the Contractor Support site:

There are three ways to solve this problem depending on how/where your EmPCalc files are downloaded and saved on your computer.

1. If your EmPCalc is saved on your computer and not a shared drive (including OneDrive), the easiest way to resolve this issue on individual files is to remove the Mark of the Web as shown here:
2. If your EmPCalcs are saved on an internal network drive or locally trusted website follow these instructions:
3. If your EmPCalc's are downloaded to a OneDrive or SharePoint site follow these instructions:

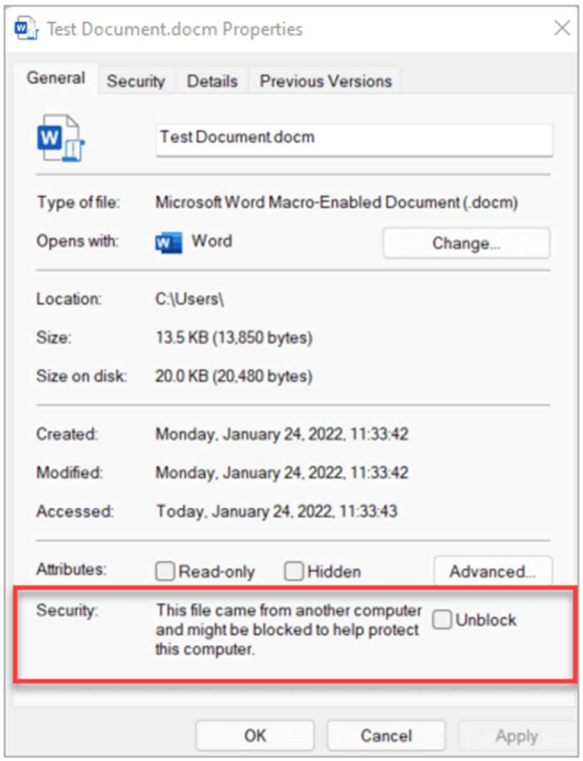
Additional information regarding this issue can be found here:

https://docs.microsoft.com/en-us/deployoffice/security/internet-macros-blocked#files-centrally-located-on-a-network-share-or-trusted-website

Guidance on allowing VBA macros to run in files you trust

Remove Mark of the Web from a file

For an individual file, such as a file downloaded from an internet location or an email attachment the user has saved to their local device, the simplest way to unblock macros is to remove Mark of the Web. To remove, right-click on the file, choose **Properties**, and then select the **Unblock** checkbox on the **General** tab.



Files centrally located on a network share or trusted website

If you have your users access files from a trusted website or an internal file server, you can do either of the following steps so that macros from those locations won't be blocked.

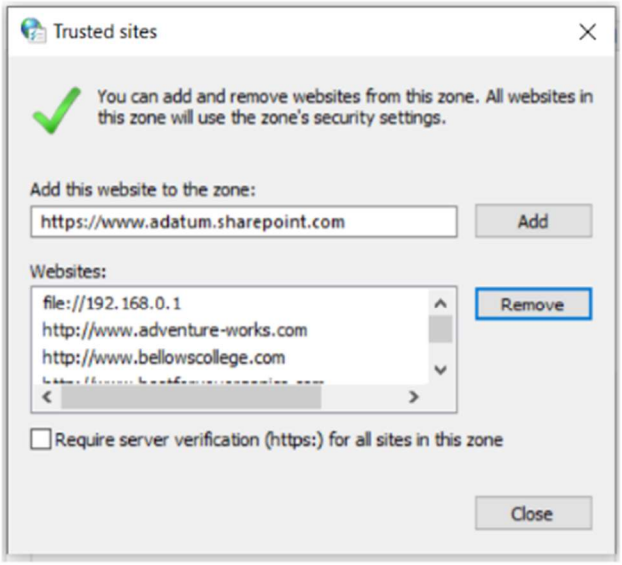
- Designate the location as a Trusted site
- If the network location is on the intranet, add the location to the **Local intranet** zone

> **Note**
>
> - If you add something as a trusted site, you're also giving the entire site elevated permissions for scenarios not related to Office.
> - For the **Local intranet** zone approach, we recommend you save the files to a location that's already considered part of the **Local intranet** zone, instead of adding new locations to that zone.
> - In general, we recommend that you use trusted sites, because they have some additional security compared to the **Local intranet** zone.

For example, if users are accessing a network share by using its IP address, macros in those files will be blocked unless the file share is in the **Trusted sites** or the **Local intranet** zone.

> **Tip**
>
> - To see a list of trusted sites or what's in the **Local intranet** zone, go to **Control Panel** > **Internet Options** > **Change security settings** on a Windows device.
> - To check if an individual file is from a trusted site or local intranet location, see **Mark of the Web and zones**.

For example, you could add a file server or network share as a trusted site, by adding its FQDN or IP address to the list of trusted sites.



If you want to add URLs that begin with http:// or network shares, clear the **Require server verification (https:) for all sites in this zone** checkbox.

Files on OneDrive or SharePoint

- If a user downloads a file on OneDrive or SharePoint by using a web browser, the configuration of the Windows internet security zone (**Control Panel** > **Internet Options** > **Security**) will determine whether the browser sets Mark of the Web. For example, Microsoft Edge sets Mark of the Web on a file if it's determined to be from the Internet zone.
- If a user selects **Open in Desktop App** in a file opened from the OneDrive website or from a SharePoint site (including a site used by a Teams channel), then the file won't have Mark of the Web.
- If a user has the OneDrive sync client running and the sync client downloads a file, then the file won't have Mark of the Web.
- Files that are in Windows known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll), and are synced to OneDrive, don't have Mark of the Web.
- If you have a group of users, such as the Finance department, that need to use files from OneDrive or SharePoint without macros being blocked, here are some possible options:
  - Have them open the file by using the **Open in Desktop App** option
  - Have them download the file to a Trusted Location.
  - Set the Windows internet security zone assignment for OneDrive or SharePoint domains to Trusted Sites. Admins can use the "Site to Zone Assignment List" policy and configure the policy to place `https://{your-domain-name}.sharepoint.com` (for SharePoint) or `https://{your-domain-name}-my.sharepoint.com` (for OneDrive) into the Trusted Sites zone.
    - This policy is found under Windows Components\Internet Explorer\Internet Control Panel\Security Page in the Group Policy Management Console. It's available under both Computer Configuration\Policies\Administrative Templates and User Configuration\Policies\Administrative Templates.
    - SharePoint permissions and OneDrive sharing aren't changed by adding these locations to Trusted Sites. Maintaining access control is important. Anyone with permissions to add files to SharePoint could add files with active content, such as macros. Users who download files from domains in the Trusted Sites zone will bypass the default to block macros.