

# Sun City Computer Club

Cyber Security SIG

April 1, 2021

**Questions, Comments, Suggestions welcomed at  
any time**

**Even Now**



- Audio recording of this session as MP4 file
- Audio recording available at link shown above

## Audio Recording In Progress

**SIG attendees are required to be members of the chartered club sponsoring that SIG.  
Sun City Community Association By-law**



**APRIL FOOL'S  
DAY**



## Blog Archive

### ▼ 2021 (13)

#### ▼ March (6)

iOS 14.4.2 Update released 26-Mar-2021

Android spyware masquerades as System Update

Android apps keep crashing?

Emergency Windows 10 updateS released today 16-Mar...

iOS update for iPhone iPad, iWatch, and MacOS

Microsoft Exchange Servers - SERIOUS vulnerabiliti...

#### ▼ February (3)

MacOS & Silver Sparrow

REALLY SOARING UTILITY BILLS?

I have been hacked, now what?

#### ▶ January (4)

### ▶ 2020 (56)

### ▶ 2019 (28)

### ▶ 2018 (57)

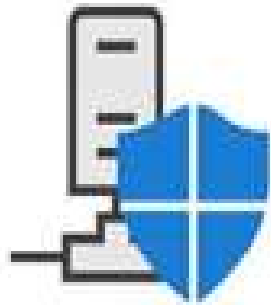
### ▶ 2017 (62)

### ▶ 2016 (16)

# Current News Blog Posts

# Automatic mitigation with Microsoft Defender

Immediate mitigation for threats taking advantage of Exchange Server vulnerabilities



The latest version of Microsoft Defender Antivirus helps mitigate Exchange Server attacks by performing these actions:

- ✓ Automatically mitigate CVE-2021-26855 via a URL Rewrite configuration
- ✓ Scan the server and reverse changes made by known threats

---

To get this automatic mitigation, enable Microsoft Defender Antivirus automatic updates, or update to detection build **1.333.747.0** or newer.

Important note: To get the latest info from Microsoft about this threat, including mitigation and investigation guidance, go to <https://aka.ms/ExchangeVulns>.



Settings



## Windows Update



### Updates available

Last checked: Today, 11:33 AM

Security Intelligence Update for Microsoft Defender Antivirus -  
KB2267602 (Version 1.333.1773.0)

**Status:** Installing - 0%

[View optional updates](#)



Pause updates for 7 days

Visit [Advanced options](#) to change the pause period



Change active hours

Currently 8:00 AM to 8:00 PM



View update history

See updates installed on your device



Advanced options

Additional update controls and settings

- Microsoft Windows 10  
Cumulative Update Preview  
3/29/2021    KB5000842

# Highlights

- Updates an issue with zoom that occurs when using Microsoft Edge IE Mode on devices that use multiple high-DPI monitors.
- Updates an issue that makes high dynamic range (HDR) screens appear much darker than expected.
- Updates an issue that causes video playback to be out of sync in duplicate mode when you use multiple monitors.
- Updates an issue that displays nothing or shows "Computing Filters" indefinitely when you filter File Explorer search results.
- Updates an issue that makes the split layout unavailable for the touch keyboard when you rotate a device to portrait mode.
- Informs users when a child account in the Family Safety plan has administrative privileges.
- Updates an issue that prevents you from closing Toast Notifications using the Close button on touchscreen devices.
- Updates an issue with 7.1 channel audio technology.
- Updates an issue that causes a device to stop working if you delete files or folders that OneDrive syncs.



## Windows 10, version 20H2

This non-security update includes quality improvements. Key changes include:

- This build includes all the improvements from Windows 10, version 2004.
- No additional issues were documented for this release.

1. SENDER EMAILS
2. info@icartservice.com
3. inform@icartservice.com
4. it@icartservice.com
- 5.
6. SUBJECTS
7. Do you want to extend your free period #####?
8. Do you want to extend your free trial #####?
9. Free period for ##### will come to the end end in 3 days
10. Free trial period for ##### ends in three days
11. Free trial period for ##### will end in 3 days
12. Your free period ##### is about to end!
13. Your free trial ##### is about to end!

- Provide ID
- Fill out this form for refund
  
- Why not? There's no link to click.

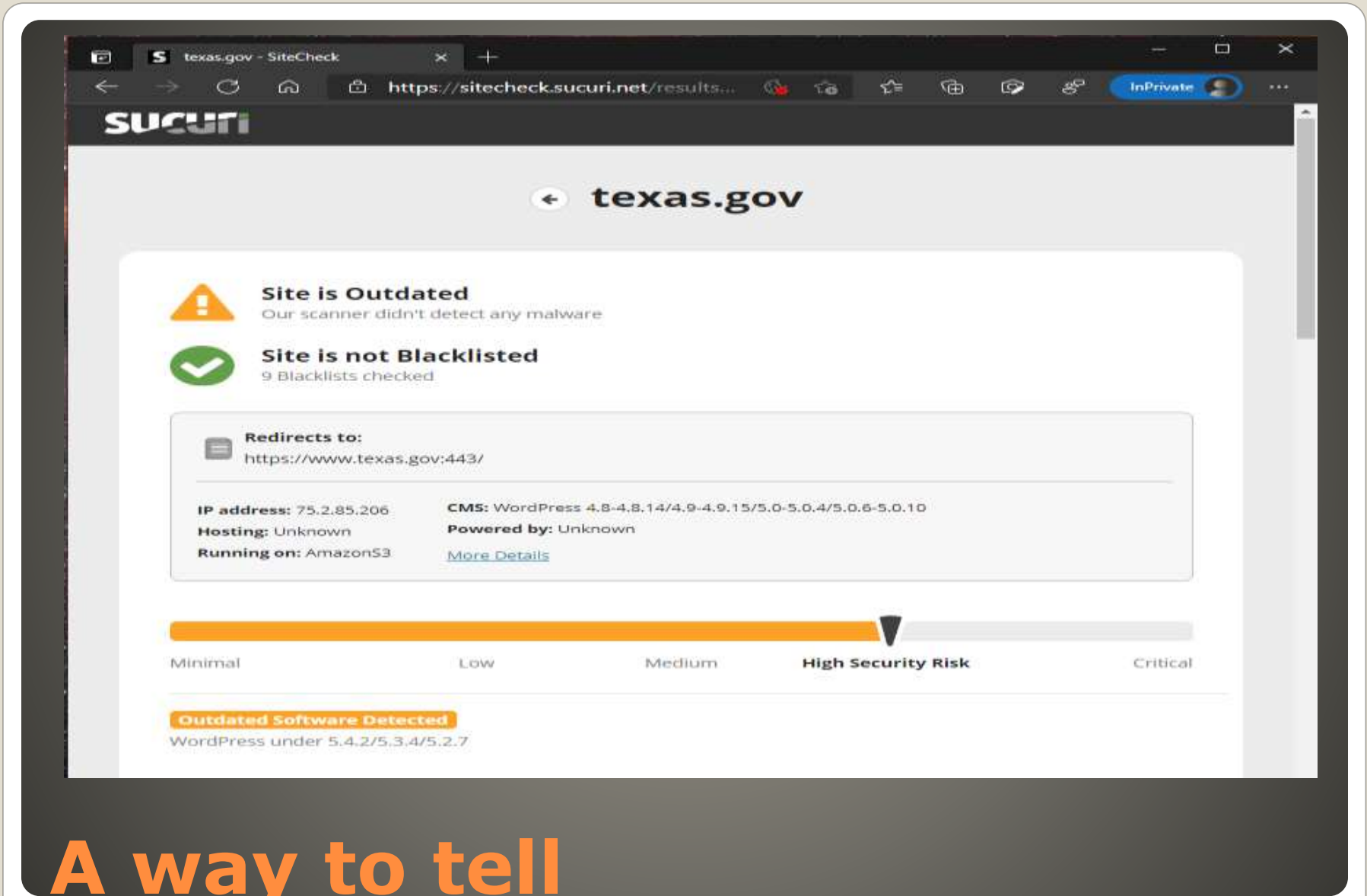
**BazarCall**

- OpenSSL CVE-2021-3449 Server crash
- SolarWinds yet again & DHS access
- Cloudflare Browser Isolation  
Rendering – visual result on user's browser
- Ubiquiti breach  
LastPass  
AWS  
Linksys, Cisco, TP-Link, etc.
- PHP
- Space probes, satellite comms,
- Roku activation fee tech support fees
- Background Intelligent Transfer Service (BITS)  
Job concept unused bandwidth

**Current Issues esoteric?**

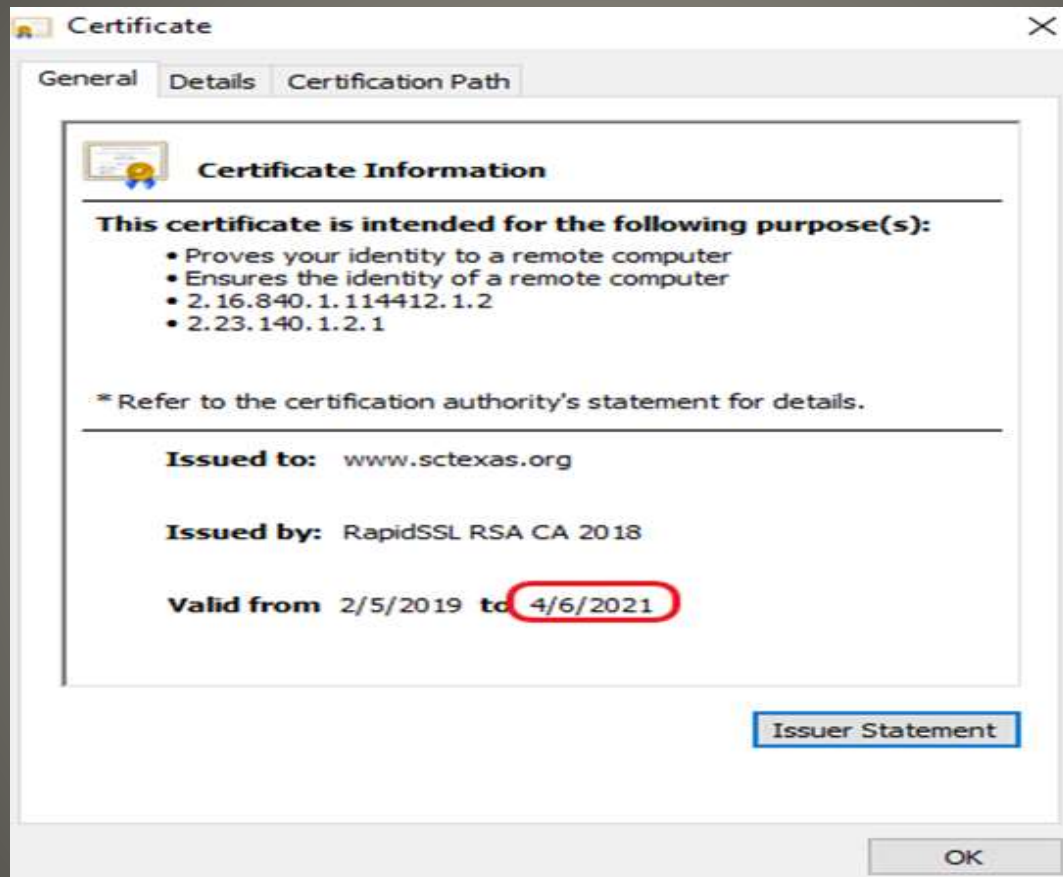
- Samba CVE-2021-20277  
CVE-2021-25833
- Windows Sandbox update
- Apple app-tracking transparency initiative  
Delayed from Sept  
block access to Advertising ID
- Lock icon  
NOT trust  
NOT Identity  
Reverse Proxy
- Exchange Server patched NOT SO Fast
- Australia Cyber Security Centre scans
- WordPress

## Current Issues



A way to tell

- Microsoft IIS 8.5 2013



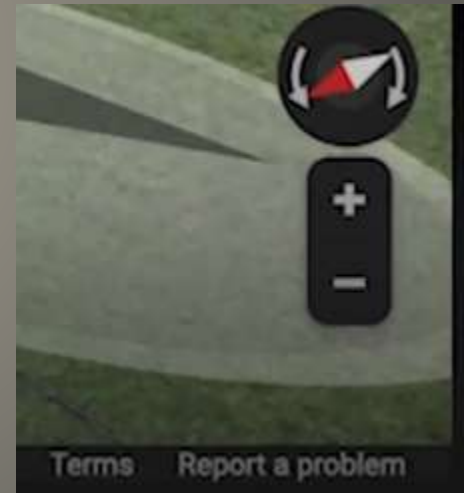
Computer Club website

# Partial Entry Forms

Get More Leads, Recover Lost Leads, Find Weak Points

Our services allow you to collect information that is filled out on a website form when the user doesn't click the "Submit" button.

- Just because
- License plate open drapes pet outside
- PERMANENT - resale
- Probably on Zillow
- Raises question – Why?



**Google street view blur my house**



- Report a Problem

Why are you reporting this image? (Please choose from one set of options.)

**Request blurring:** What would you like us to blur?

- A face
- My home
- My car / a license plate
- A different object

- Provide “why?”
- eMail address
- Submit

**Google Street View Blur house**





**US Strategic Command** ✓ @... · 31m

;l;;gmlxzssaw

1,557 6,664 8,549

- Bank warning fake check scams
- Ransomware “got insurance?” CNA
- US cyber czar  
National Cyber Director  
National Defense Authorization Act
- Google takes down counterterrorism operation
- Congressional hearings  
SolarWinds attacks from within US  
dozens cyber operations 2020 elections
- Zoom, etc. Control Notifications!
- Cyber attack forces live TV broadcast off the air

## Current Issues

- Federated Learning of Cohorts
- Gmail 1.5Billion Outlook 400Million
- SPAM control – not bad
- Creepy line
- Apple IDFA ID for Advertisers
- Apple ATT App Tracking Transparency
- 99% say NO
- China Anonymization ID (CAID)

**Google FLoC**

- “Technology does not need vast troves of personal data, stitched together across dozens of websites and apps, in order to succeed. Advertising existed and thrived for decades without it. If a business is built on misleading users, on data exploitation, on choices that are no choices at all, then it does not deserve our praise. It deserves reform.”

**Tim Cook, Apple CEO**

- Cohort ID
- Medical implies medical
- Political implies political
  
- Advertisers have subsidized a lot
  
- Browsers fit for purpose
  
- What if law firms could only show a limited number of ads?


- Yet another trace of past activity
- DNS cache poisoning
- Varied and sundry

**DNS cache**






All Apps Documents Web More ▾


Best match

 Windows PowerShell  
App


Apps

-  Windows PowerShell ISE >
-  Windows PowerShell ISE (x86) >
-  Windows PowerShell (x86) >





Search the web

 powers - See web results >

Settings (3+)



Windows PowerShell  
App

-  Open
-  Run as Administrator
-  Run ISE as Administrator
-  Windows PowerShell ISE

▾

**Clean DNS**

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\WINDOWS\system32>
```

**Clean DNS**

- `sudo killall -HUP mDNSResponder`

**MacOS**

# • “TrustRecords” registry

HKCU:\SOFTWARE\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords

HKCU:\SOFTWARE\Microsoft\Office\16.0\Excel\Security\Trusted Documents\TrustRecords

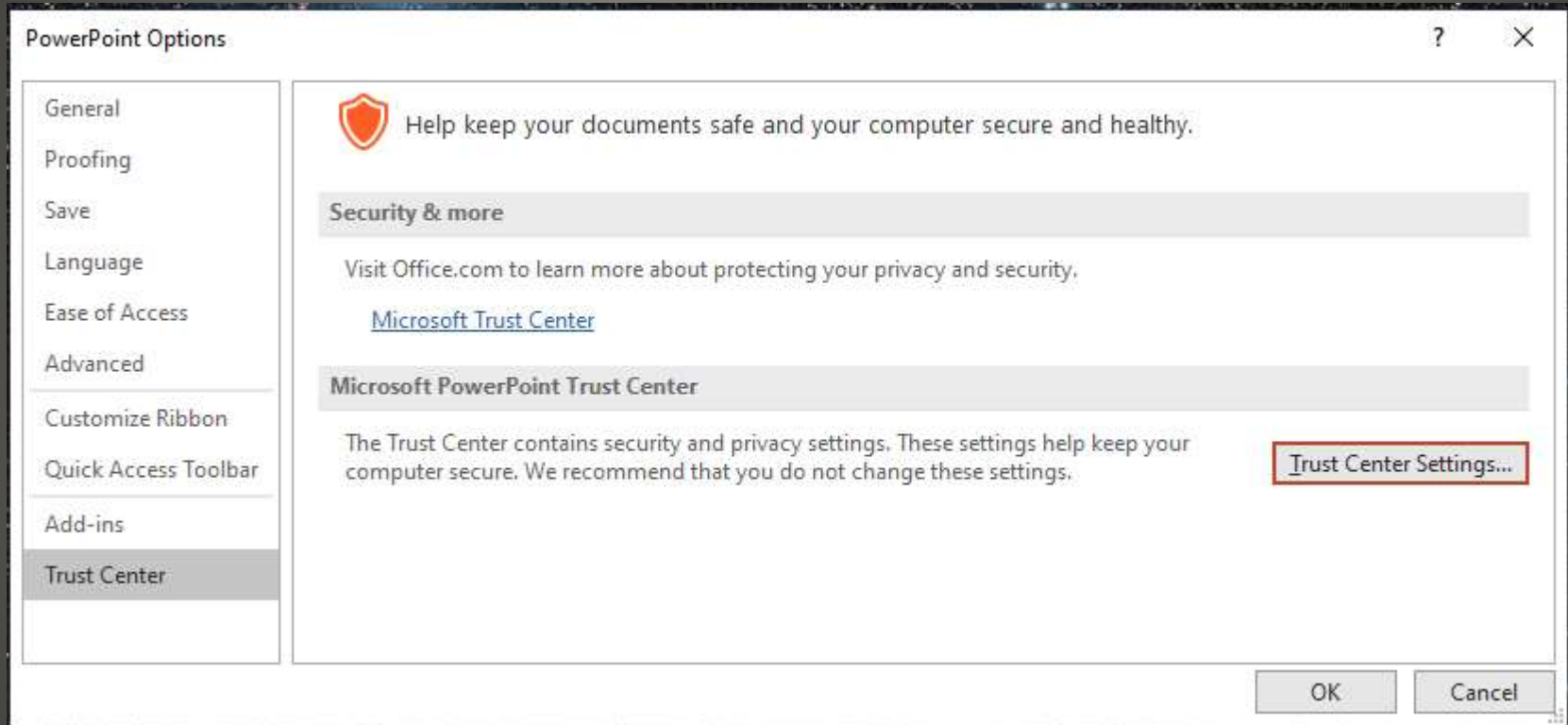
HKCU:\SOFTWARE\Microsoft\Office\16.0\PowerPoint\Security\Trusted Documents\TrustRecords

Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Office\16.0\Excel\Security\Trusted Documents\TrustRecords

Name	Type	Data
(Default)	REG_SZ	(value not set)
%USERPROFILE%\Downloads\Invoice%2038421.xls	REG_BINARY	ee f7 4b 78 75 1f d7 01 00 60 ee 78 de ff ff ff 12 16 9b 01 01 00 00 00
%USERPROFILE%\Downloads\invoice%2058633.xls	REG_BINARY	43 78 7f bb 08 21 d7 01 00 60 ee 78 de ff ff ff 58 21 9b 01 ff ff ff 7f
%USERPROFILE%\Downloads\Invoice%2094377.xls	REG_BINARY	1e 63 55 9c 5e 1f d7 01 00 60 ee 78 de ff ff ff 6e 15 9b 01 01 00 00 00

# Microsoft Office Macro

- Suggest registry search TrustRecords



**Microsoft Office Macros**

Trust Center

? X

- Trusted Publishers
- Trusted Locations
- Trusted Documents
- Trusted Add-in Catalogs
- Add-ins
- ActiveX Settings
- Macro Settings**
- Protected View
- Message Bar
- File Block Settings
- Privacy Options
- Form-based Sign-in

Macro Settings

- Disable all macros without notification
- Disable all macros with notification
- Disable all macros except digitally signed macros
- Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

- Trust access to the VBA project object model

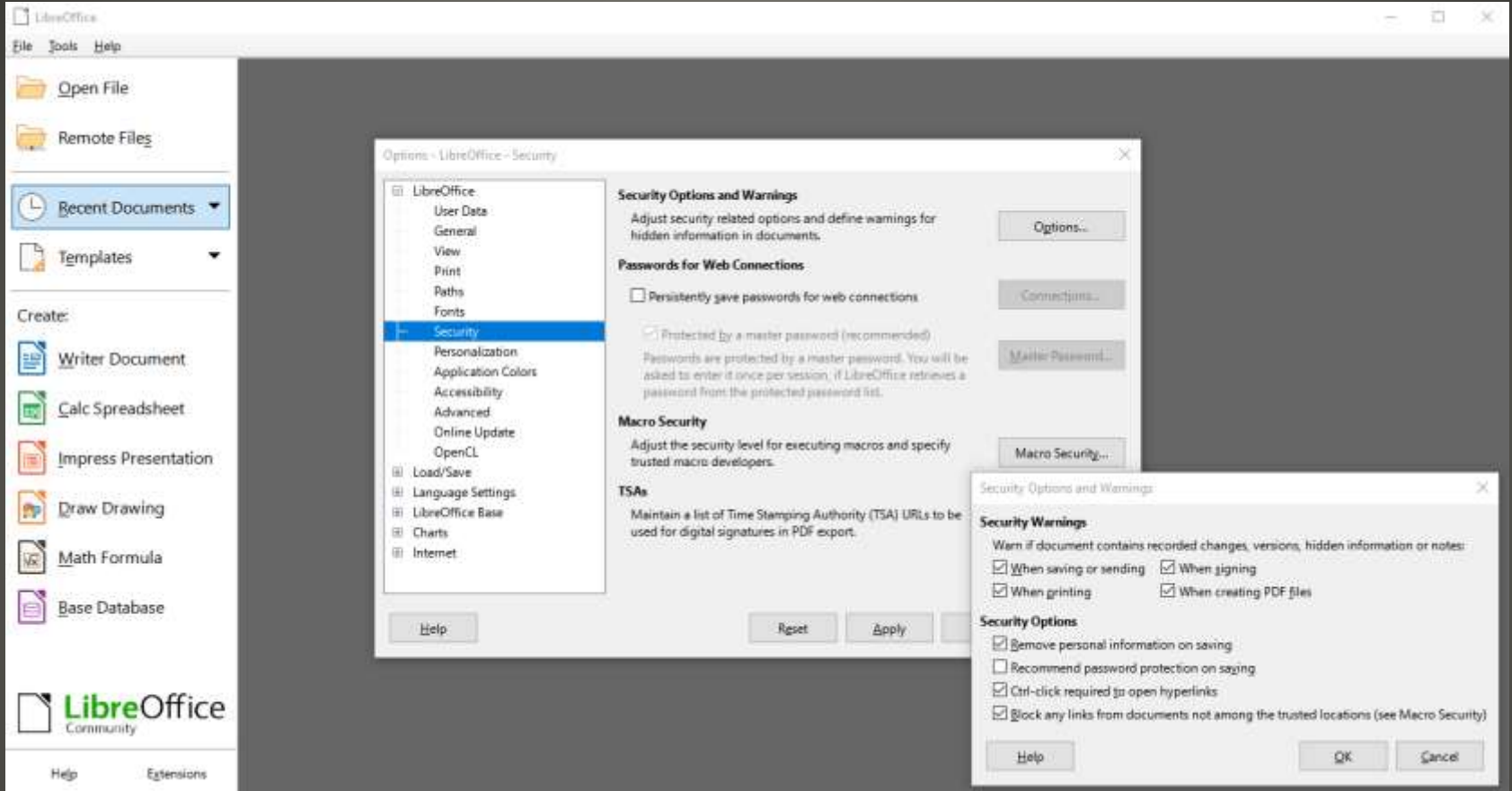
OK

Cancel

# Trust Center Microsoft Office

- Rightmost value allowed macro to run  
00 => Open for editing  
7F => Allow macro to run

**Macros**



# Libre Office Macros





### Security Warnings

Warn if document contains recorded changes, versions, hidden information or notes:

- When saving or sending
- When signing
- When printing
- When creating PDF files

### Security Options

- Remove personal information on saving
- Recommend password protection on saving
- Ctrl-click required to open hyperlinks
- Block any links from documents not among the trusted locations (see Macro Security)

Help

OK

Cancel



This document contains macros.

Macros may contain viruses. Execution of macros is disabled due to the current macro security setting in Tools - Options - LibreOffice - Security.

Therefore, some functionality may not be available.

OK

LibreOffice - Security Warning



**/home/natstan/MacroTest/TestMacro.ods**

The document contains document macros.

Macros may contain viruses. Disabling macros for a document is always safe. If you disable macros you may lose functionality provided by the document macros.





 Help


Disable Macros

Enable Macros

- Macros
- Helpful
  - Greatly extends function of office apps
- Harmful
  - Greatly extends function of office apps
- Scripting
  - Any/everything an developer needs
  - Any/everything an attacker needs

Check Control

2      07:06

 Function acquirable

Close message

The high-beam assistant can be acquired in the ConnectedDrive Store. The function reduces the load on the driver during darkness by automatically turning the high beam on and off in the case of oncoming vehicles and vehicles ahead.

## High Beam Assistant



Switching between low beam and high beam can be done automatically in your BMW, thanks to the High Beam Assistant.

**> Details**

starting at £ 160.00

**Offers and prices**



Recipes...for... cookies

vieM

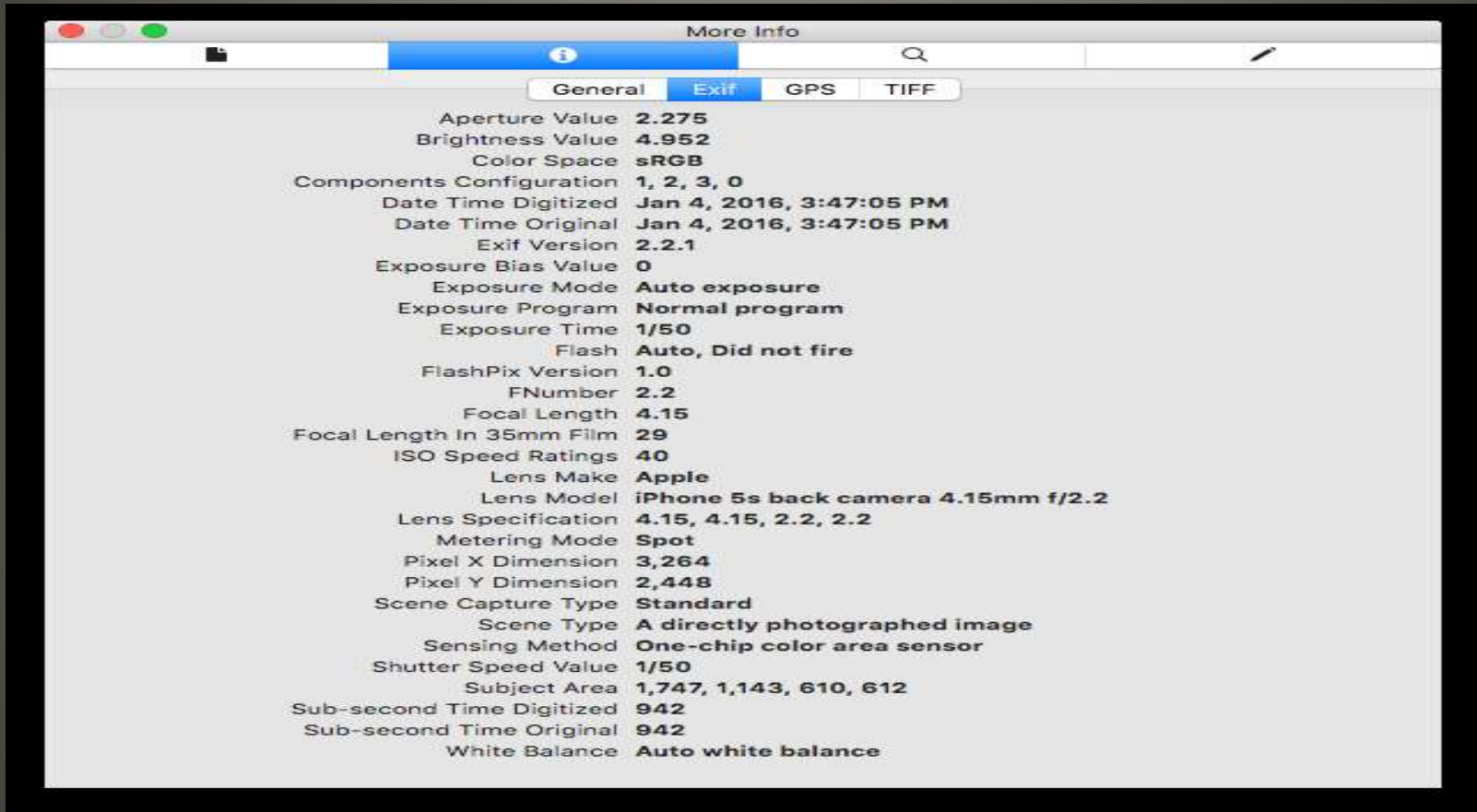
## WEB BROWSER SAFETY TIPS

- Use pop-up blockers. Pop-up rules can be changed in a browser's "Settings" or "Options" menu
- Look for the "S" after http in the web address, indicating the website is secure
- Look for a padlock in the address bar. The padlock indicates secure mode.
- Make sure automatic updates are turned on and working efficiently.
- Beware of using the autofill and built-in password management feature in your browser. Autofill fills in the fields on a form automatically, according to the information that the user has previously used. 13



**Semantics Government Safe**

- EXchangeable Image File metadata



Smart device Photos EXIF sharing





# EXIF metadata Android

- Helpful <-> Harmful
- Helpful
  - Organize
  - Photo data
  - Copyright
- Harmful
  - Privacy
  - Tracking
- Part of photo file
  - Removed in format conversion, upload to social media, editing programs
- Not removed with filesharing, eMail, SMS, etc.
- Remove location permissions for camera app(s)

**EXIF**

Preview	Metadata		
<i>f/</i> 10.0	1/250	6000 x 4000	
	+0.67	68.16 MB	—
	ISO 200	Untagged	RGB
> File Properties			
> IPTC Core			
> IPTC Extension			
∨ Camera Data (Exif)			
Exposure Mode	Auto		
Brightness Value	9.35		
Sensitivity Type	Standard output sensitivity (SOS)		
Focal Length	18.0 mm		
Focal Length in 35mm Film	27.0 mm		
Lens	XF18-135mmF3.5-5.6R LM OIS WR		
Max Aperture Value	f/3.5		
Date Time Original	5/21/2018, 8:21:56 AM		
Flash	Did not fire		
Metering Mode	Average		
Custom Rendered	Normal Process		
White Balance	Auto		
Scene Capture Type	Standard		
Sharpness	Normal		
Sensing Method	One-chip sensor		
File Source	Digital Camera		
Make	FUJIFILM		
Model	X-T2		
Body Serial Number	XXXXXXXXXX		
Lens Specification	18-135mm f/3.5-5.6		
Lens Make	FUJIFILM		
Lens Serial Number	XXXXXXXXXX		
∨ GPS			
Latitude	37,31.7232N		
Longitude	111,59.3713W		
Altitude	1791.72 m		

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs,  
Presentations, FirstTime, classes  
Cyber Security SIG meetings, NEWSBLOG  
Internet

- Questions, suggestions, comments?

**SCCCCyber@gmail.com**



QUESTIONS ?

