



PLATEAU PC USERS GROUP, INC GAZETTE



October 2026

Published by the Plateau PC Users Group, Inc. 221 Tomlon Road Crossville TN 38555
"JOIN US FOR FUN AND LEARNING AT CROSSVILLE'S COMPUTER CLUB"

October 2026 Volume 32 Issue 10

This Month's General Meeting
Tuesday, October 13, 2026
will start at 3:00 P.M. @
FFG Christ Lutheran Church

October 13th Presentation
@ 3:00 P.M.

Introduction to LINUX

Today's program will be an
Introduction to LINUX and
why it might apply to you.



After the demonstration, we will
have an extended open question/
discussion session.



Saturday, October 31, 2026

Inside This Issue

Club information and Phone numbers	Page 2
Cool Tips & Sites: Microsoft made an app just to force Bing into your browser	Page 3
How to fix Outlook Keeps Asking for Your Password	Page 4
How to Secure Your Google Account in 30 Minutes	Page 9
Microsoft Word Tips	Page 13
PPCUG 2026/27 Application for Membership.	Page 15
November 2026 Calendar.	Page 16

Please Note: All Meetings will now be on the second
Tuesday of each month. Starting at 3:00 P.M.

Location: Christ Lutheran Church
481 Snead Drive, Fairfield Glade TN

Join the Club!

Anyone interested to attend the general meeting or any of the SIG meetings as a guest will be charged \$3.00 per person for any or all meetings in that month. Afterwards, you are encouraged to become a member of the Plateau PC Users Group. Our Club cannot exist without you, the members.

Membership Dues

Our annual dues are now payable July 1st. of each year. Annual dues are \$24 per single person / \$30 per family. Persons/families joining during the fiscal year have dues payable as follows:

<u>Join In</u>	<u>July - Sept</u>	<u>Oct - Dec</u>	<u>Jan - Mar</u>	<u>Apr - June</u>
Single	\$24	\$18	\$12	\$6
Family	\$30	\$22	\$15	\$7

BOARD OF DIRECTORS DISCLAIMER

All members of the Plateau PC Users Group are willing to help one another in the area of advice and tutorial instruction over the phone. If you should require more involved services or instruction, we have a few members who are very knowledgeable in several areas. As a responsible consumer, it is up to you to discuss, before retaining a member, any and ALL charges for repair services and time consuming tutorial activities.

It is not the desire of this Board of Directors to set fees for individuals for services rendered, nor the responsibility to intervene between members who enter into a contract among themselves.

The GAZETTE is published using the following: Microsoft Word, Microsoft Publisher, and Microsoft Windows. The Gazette is the monthly newsletter of the Plateau PC Users Group, Inc.

DISCLAIMER: No warranty, express or implied, is made by the PPCUG, the Gazette editorial staff or its contributing editors. This extends to all losses incidental or consequential from the use or non-use of any information in any issue of the Gazette.

All images used in the newsletter, website, blogs, class materials or handouts ("media") are obtained from a "free use" source, preferably images that have been released as "CCO Public Domain".

PPCUG, Inc. 2026-2027 Board Members



President	George Sengstock	(224) 760-3948
Vice-President/	Charlie Merrick	(931) 210-8013
Treasurer	Richard Del Frate	(931) 456-2251
Secretary	Richard Del Frate	(931) 456-2251
Membership	George Sengstock	(224) 760-3948
Publicity	George Sengstock	(224) 760-3948
Gazette Editor	Gordon Botting	(931) 456-2184
APCUG Rep	George Sengstock	(224) 760-3948
Equipment Custodian	Bob Willis	(931) 456-6511
Webmaster	Alan Baker	(931) 239-0877

Directors at Large

Alan Baker	Gordon Botting Brick	Joe Brickweg
Barbara Duncan	Richard Del Frate	Bob Willis



Printed by, Business Equipment Clinic
539 West Ave. Suite 101 Crossville TN 38557

Cool Tips and Sites

Microsoft made an app just to force Bing into your browser.

You expect this kind of thing from shady free software, not from Microsoft itself. But here we are.

Microsoft has quietly released a standalone app called "**Microsoft Recommended Search Settings**" whose entire purpose is to switch your browser's search engine to Bing.

It's a roughly 22MB download hosted on Microsoft's own servers, and it works on Chrome, Firefox, and Brave. Once run, it installs a "Microsoft Bing Homepage & Search" extension with the switch-to-Bing toggle already ticked, then sends you off to Microsoft Rewards.

The cheeky part: if you later try to set Chrome back to Google, it pops up a nag overlay begging you not to.

The big picture:

To be fair, this isn't malware and it isn't forced on you through Windows Update. Microsoft's line is that it's optional and needs your consent. But it behaves exactly like the browser-hijacking adware we tell people to avoid, and it's the kind of thing that lands on a PC because someone clicked a "recommended settings" prompt without reading it. When the company that makes your operating system starts shipping software like this, it's worth knowing how to undo it.

Here's how to get rid of it.

First, open your browser's extensions page (Chrome, Firefox, or Brave) and remove the "Microsoft Bing Homepage & Search" extension.

Then reset your search engine and homepage back to what you want in your browser settings.

Finally, check Settings, Apps, Installed apps in Windows and uninstall "Microsoft Recommended Search Settings" if it's there. Done. Your browser is yours again.

**** Visit the PPCUG Website ****

At: www.PPCUGinc.com Read all about our club activities and scheduled monthly meetings, also current and past issues of the Gazette Newsletter. Links also to the Meeting Handouts on past presentations.

Send your comments and suggestions to the PPCUG Webmaster,
Alan Baker @ jackal33980@gmail.com (931) 239-0877

How to Fix Outlook Keeps Asking for Your Password

Dellenny

by John Edward

There are few things more frustrating than opening Outlook, getting ready to check your email, and seeing the same password prompt again and again. You enter the correct password, click **Sign In**, and everything seems fine until Outlook asks for your password once more.

If this keeps happening, you're not alone. The **"Outlook keeps asking for your password"** problem can happen in Microsoft Outlook on Windows for several reasons.

Sometimes it's caused by incorrect saved credentials, an outdated Outlook installation, a damaged profile, authentication problems, or issues with your Microsoft 365 account.

The good news is that you usually don't need to reinstall everything to fix it. In this guide, we'll walk through practical solutions, starting with the easiest ones and moving toward more advanced fixes.

Why Does Outlook Keep Asking for Your Password?

Before changing anything, it helps to understand why Outlook might repeatedly request your password. One common reason is that Outlook has stored an outdated password. For example, if you recently changed your Microsoft account or email password, Windows may still have the old credentials saved. Outlook tries to use them, fails authentication, and asks you to sign in again.

Other possible causes include:

- Corrupted Windows or Outlook credentials
- An outdated version of Outlook
- Problems with your Outlook profile
- Incorrect account settings
- Microsoft 365 authentication issues
- Cached login information
- Network or connectivity problems
- An account password that has expired
- Security software interfering with authentication
- Problems with modern authentication

The right solution depends on what's causing the repeated prompt, so it's worth working through the fixes one at a time.

(Continued on page 5)

(Continued from page 4)

1. Check Your Internet Connection

Start with something simple: make sure your internet connection is working properly. Outlook needs to communicate with your mail server or Microsoft 365 services to authenticate your account. If your connection keeps dropping, Outlook may repeatedly ask you to sign in.

Try opening a few websites in your browser. If your connection appears unstable, restart your router or switch to another network temporarily. If the internet works normally and Outlook still keeps asking for your password, move on to the next step.

2. Make Sure Your Password Is Actually Working

It sounds obvious, but it's worth checking whether your email password works outside Outlook. Open your email provider's official sign-in page and try logging in with the same email address and password.

If you can't sign in there either, the issue probably isn't Outlook itself. You may need to reset your password or resolve an account-related problem first.

If you can sign in successfully through the browser but Outlook continues asking for your password, the problem is more likely related to Outlook, Windows credentials, or the local account profile.

3. Remove Old Credentials From Windows

One of the most common reasons Outlook repeatedly asks for a password is an outdated credential stored in Windows.

Windows Credential Manager stores login information for various applications and services. If Outlook is using an old password, removing the saved credential can force Outlook to request fresh authentication. To check your credentials:

1. Close Outlook completely.
2. Open **Control Panel**.
3. Select **Credential Manager**.
4. Click **Windows Credentials**.
5. Look for entries related to Outlook, Microsoft Office, Microsoft 365, or your email account.
6. Remove the relevant outdated credentials.
7. Restart your computer.
8. Open Outlook again and sign in when prompted.

Be careful when deleting credentials. Don't remove unrelated entries unless you know what they are used for.

(Continued on page 6)

(Continued from page 5)

Once Outlook has a chance to authenticate again, the repeated password prompt may disappear.

4. Update Microsoft Outlook

Running an older version of Outlook can sometimes cause authentication problems.

Microsoft regularly releases updates that improve security, compatibility, and account authentication. If Outlook hasn't been updated for a while, check for available updates.

If Outlook opens:

1. Open Outlook.
2. Select **File**.
3. Choose **Office Account**.
4. Select **Update Options**.
5. Click **Update Now**.

Allow the update to finish and restart Outlook.

If you're using Microsoft 365, keeping Office applications updated is particularly important because account authentication methods and security requirements can change over time.

5. Restart Outlook and Your Computer

It may sound like a basic suggestion, but don't underestimate it.

Outlook and Windows can occasionally get stuck with an authentication session that isn't behaving correctly. Closing Outlook and restarting Windows can clear temporary processes and refresh your connection.

Make sure Outlook is completely closed before restarting. If necessary, check Task Manager to confirm that no Outlook process is still running.

After restarting your computer, open Outlook and check whether the password prompt appears again.

6. Check Outlook's Account Settings

Incorrect account configuration can also lead to repeated password requests.

Open Outlook and go to your account settings. Depending on your Outlook version, the exact menu names may differ.

Check that the email address and account information are correct. If you're using a company or Microsoft 365 account, your organization's administrator may have specific authentication requirements.

Avoid changing server settings randomly, especially if you're using a work or school account. Incorrect settings can create additional connection problems.

(Continued on page 7)

(Continued from page 6)

If your organization manages your Outlook account, contacting the IT administrator may be the quickest way to confirm whether there are account-side authentication changes.

7. Create a New Outlook Profile

If your current Outlook profile has become corrupted, creating a new profile can often resolve persistent login problems.

A profile contains account and configuration information that Outlook uses to connect to your mailbox. If that information becomes damaged, Outlook may behave unpredictably—including repeatedly asking for your password.

To create a new profile:

1. Close Outlook.
2. Open **Control Panel**.
3. Search for **Mail**.
4. Open the Mail settings.
5. Select **Show Profiles**.
6. Choose **Add**.
7. Give the new profile a name.
8. Add your email account.
9. Set Outlook to use the new profile.
10. Open Outlook again.

If the new profile works normally, your original profile may have been the source of the problem.

8. Repair Microsoft Office

Another option is to repair your Microsoft Office installation.

Windows provides built-in repair options that can fix damaged Office files without requiring you to completely uninstall the software.

Go to:

Settings → Apps → Installed Apps

Find Microsoft 365 or Microsoft Office, select the available options, and look for **Repair**.

Depending on your installation, you may see options such as **Quick Repair** and **Online Repair**.

It's generally sensible to try Quick Repair first. If the problem continues, Online Repair may provide a more thorough repair, although it can take longer and may require an internet connection.

(Continued on page 8)

(Continued from page 7)

9. Check Whether Your Password Has Recently Changed

Did you recently change your Microsoft, Microsoft 365, or email password?

If yes, this is an important clue.

Other Microsoft applications on your computer may still have cached authentication information from before the password change. Outlook could therefore continue trying to authenticate with an outdated session.

Signing out of Microsoft applications and signing back in can sometimes refresh the authentication process.

If this is a work or school account, your organization's security policies may also require additional verification, such as Microsoft Authenticator or another multi-factor authentication method.

10. Check Multi-Factor Authentication

Modern Microsoft accounts often use multi-factor authentication (MFA).

If MFA is enabled and the authentication process isn't completing correctly, Outlook may appear to be stuck in a sign-in loop.

Check whether you are receiving authentication requests on your phone or authentication app. Also make sure your account isn't waiting for an approval or verification step.

If your organization uses Microsoft Entra ID or another managed identity system, the IT administrator may need to check the account's authentication status.

11. Run Outlook Without Add-Ins

Sometimes an Outlook add-in can interfere with normal operation.

You can test Outlook in Safe Mode to determine whether an add-in is contributing to the issue.

Press **Windows + R**, enter:

outlook /safe

and press Enter.

If Outlook works normally in Safe Mode and stops repeatedly asking for your password, an add-in may be involved.

You can then disable unnecessary add-ins and restart Outlook normally.

12. Remove and Add the Account Again

If you've tried the previous solutions and Outlook still keeps asking for your password, removing the affected account from Outlook and adding it again may help.

Before doing this, make sure you know your account credentials and understand whether your mailbox is hosted on Microsoft 365, Exchange, IMAP, or another service.

For business accounts, it's also a good idea to confirm the correct configuration with your IT administrator before removing the account

How to Secure Your Google Account in 30 Minutes

- by John Edward

A compromised Google account is rarely just an email problem. For many professionals, it is a gateway to Google Drive, Calendar, Chrome-synced data, cloud consoles, source-code repositories, SaaS applications, and sensitive business conversations.

The good news: you can significantly improve your account security in about 30 minutes. You do not need a security background or a collection of expensive tools. You need to review the right settings in the right order: authentication, recovery, active sessions, third-party access, and suspicious activity.

Here is a practical 30-minute checklist for securing a personal Google Account.

0–5 Minutes: Check Your Security Status

Start with Google's **Security Checkup**. It brings several important account controls into one place and can surface issues that deserve immediate attention.

Look for:

- Recent security events you do not recognize
- Devices currently signed in
- Recovery phone numbers and email addresses
- Password problems
- Third-party applications with account access

Do not automatically dismiss an unfamiliar device or event. First, determine whether it belongs to you.

For example, a Windows PC might appear under a device name you do not recognize even though it is your machine. Likewise, a recent sign-in from another location could be legitimate if you are traveling or using a corporate VPN.

The goal is not to eliminate every unfamiliar label. It is to establish whether the activity is expected.

If you find an event you genuinely do not recognize, treat it seriously. Change your password and review your authentication methods before continuing with the rest of the checklist.

5–12 Minutes: Strengthen Your Authentication

Your password is only one layer of account security.

Google supports several stronger authentication options, including two-step verification and passkeys. For accounts containing business, financial, development, or sensitive personal information, enabling an additional authentication factor should be a baseline control.

Turn on 2-Step Verification

Two-step verification requires an additional verification step when Google needs to confirm your identity.

(Continued on page 10)

(Continued from page 9)

Depending on your account and configuration, available methods can include:

- Google prompts
- Authenticator-generated verification codes
- Security keys
- Passkeys
- Other supported verification methods

A practical approach is to avoid relying on a single authentication method. Keep a recovery method available in case your primary device is lost, replaced, or unavailable.

Consider a Passkey

Passkeys use cryptographic credentials rather than asking you to enter a traditional password each time. They are designed to resist phishing because authentication is tied to the legitimate website or service rather than relying on a password that can be copied and reused.

For users with compatible devices, adding a passkey can reduce dependence on passwords while strengthening protection against common credential-theft attacks.

Do Not Reuse Your Google Password

If your Google password is used anywhere else, change that.

Password reuse creates a dangerous dependency: a breach at an unrelated website can expose credentials that attackers then try against your Google account.

For a unique password, use a reputable password manager rather than trying to invent and remember dozens of complex passwords.

12–17 Minutes: Verify Your Recovery Options

Strong authentication does not help much if your recovery information is outdated.

Open your Google Account's recovery settings and verify that the available recovery methods actually belong to you.

Check:

- Recovery phone number
- Recovery email address
- Account contact information
- Devices you regularly use for authentication

A recovery email should be protected independently. If your recovery address uses the same compromised credentials or is otherwise inaccessible, it provides little practical protection.

This is particularly important for IT professionals and developers. A Google identity may be connected to GitHub, cloud services, vendor portals, monitoring systems, documentation, and internal collaboration platforms. Losing access can become an operational problem, not just a personal inconvenience.

(Continued on page 11)

(Continued from page 10)

Do not add a recovery method you cannot reliably access. The objective is controlled recovery, not simply having more information attached to the account.

17–22 Minutes: Review Signed-In Devices

Next, inspect the devices currently associated with your account.

Look for old:

- Laptops
- Smartphones
- Tablets
- Browsers
- Workstations
- Shared or borrowed computers

If you no longer use a device, sign it out where appropriate.

This is easy to overlook. People replace phones, upgrade laptops, reinstall browsers, or leave organizations without revisiting the sessions associated with their Google identity.

An old session represents unnecessary exposure.

If a device is unfamiliar and you cannot establish that it is yours, investigate it rather than assuming it is harmless.

For a work account, coordinate with your organization's identity or security team when necessary. Google Workspace administrators may have additional controls and visibility that individual users do not.

22–26 Minutes: Remove Unnecessary Third-Party Access

OAuth makes it convenient to connect applications to your Google Account. It also creates another area worth auditing.

Open the section showing applications and services that have access to your account.

Ask three questions for every unfamiliar or unused integration:

- 1. What application is this?**
- 2. Why did I grant it access?**
- 3. Does it still need that access?**

If you stopped using an application months ago, revoke its access.

Pay particular attention to applications with broad permissions. An integration that can access Drive files, Gmail data, contacts, or other sensitive information deserves more scrutiny than a service with a narrow

(Continued on page 12)

(Continued from page 11)

permission scope.

Revoking unused access is a simple form of attack-surface reduction.

It also has a useful operational benefit: your account becomes easier to understand. When an incident happens, fewer integrations mean fewer places to investigate.

26–30 Minutes: Review Recent Security Activity

Finish by checking recent security activity again.

Look for:

- Password changes you did not make
- New device sign-ins
- Changes to recovery information
- New authentication methods
- Unexpected application connections
- Suspicious login attempts

If something looks wrong, do not try to “clean it up” while leaving the underlying credentials unchanged. Change the password, strengthen authentication, review sessions, and investigate connected applications.

What to Do If You Find a Suspicious Sign-In

If you believe someone else accessed the account, prioritize containment.

First, secure the account using Google’s account-security controls. Then review recent activity and connected services for additional changes.

If the account is used for work, involve your organization’s security or IT team. They may need to investigate related accounts, revoke sessions, review audit logs, or check for unauthorized access to business data.

For developers and cloud engineers, also consider whether the Google identity is associated with infrastructure or developer tooling. A compromised identity can have consequences well beyond Gmail.

A Simple 30-Minute Google Account Security Checklist

Save this checklist for your next security review:

- Run Google Security Checkup
- Review recent security events
- Enable or verify 2-Step Verification
- Add a passkey if appropriate

(Continued on page 13)

(Continued from page 12)

- Use a unique Google password
- Verify recovery email and phone
- Review signed-in devices
- Sign out of obsolete devices
- Audit third-party application access
- Remove unused integrations
- Review security activity again

The important part is not completing a giant security audit. It is eliminating obvious weaknesses before they become incidents.

The Next Step: Turn 30 Minutes Into a Routine

Account security should not be a one-time project.

Set a recurring reminder to review your Google Account every few months, particularly after changing phones, replacing computers, leaving a job, installing unfamiliar software, or responding to a suspected phishing attempt.

For organizations, take the same principle further. Individual account hygiene should sit alongside centralized identity controls, strong authentication policies, device management, least-privilege access, logging, and incident-response procedures.

For an individual Google Account, though, you can accomplish a surprising amount in half an hour. Start with authentication. Verify recovery. Remove stale devices and integrations. Then investigate anything you cannot explain.

Thirty focused minutes can turn a neglected account into a significantly better-protected one.

Dawn Bjork-

Microsoft Word Tips & Tricks **Microsoft Word**

Quick Overview:

Microsoft Word includes several automatic formatting features designed to save time, but they can sometimes interfere with how you want a document to look.

Have you ever typed something in Microsoft Word only to have Word change it automatically? Maybe a numbered list appeared when you didn't want one, text was reformatted, or a website or email address suddenly became a hyperlink.

These automatic features are intended to make document creation easier, but they can also get in the way. Fortunately, you can customize many of these settings, so Word works the way you want it to.

(Continued on page 14)

In this article, you'll discover a few simple settings that give you more control over automatic formatting in Microsoft Word.

Why Text Automatically Changes in Word

Does it seem like Word randomly changes the capitalization or spelling of text in a document? **AutoCorrect** is to blame. As the name indicates, AutoCorrect automatically corrects the spelling of commonly misspelled words but also makes other changes, including capitalizing the first letter in a sentence, table cell, or line of text. To review your choices and stop annoying automation in Word:

1. Pick **File > Options**.
2. Select **AutoCorrect Options** from the **Proofing** category.
3. Choose the **AutoCorrect** tab (Word 365 screen shown) and uncheck any option that gets in the way of adding your text.

How to Stop Automatic Outlines & Numbered Lists You Don't Want

Have you ever tried to create your own numbered list or outline with letters and then watched the numbering or formatting change once you press **[Enter]** for the next line? This is a huge annoyance if you want to build your own custom layout for an outline rather than working with the choices in Word.

Do you type your email address or website into a document and then watch as it suddenly changes to blue underlined text (a hyperlink)? Do you ever enter fractions or quotes that automatically re-format?

You are a victim of **AutoFormat As You Type**, a common Word ailment. Although some of these options can be helpful, turn them off if they get in the way of your work.

To customize Word so that it works for you and not against you:

1. Choose **File > Options**.
2. Pick **AutoCorrect Options** from the **Proofing** category.
3. Choose the **AutoFormat As You Type** tab (Word 365 screen shown) and uncheck any option that gets in the way of typing your text. Choices include smart quotes (different open and close quotes), fractions, hyperlinks to websites and email addresses, and automatic numbering.

I recommend you uncheck all of the options in the last two sections, including **Automatic numbered lists**. You can still turn on the automatically numbered list any time *you* want. If you work with a lot of multi-level outlines and lists, you'll want to keep the choice to **Set left- and first-indent with tabs and backspaces** found in the bottom section. Turn off choices in the 1st section as desired.

Pick **OK** to finish.

Automatic numbered and bulleted lists and outlines can still be created from the **Home** tab (Paragraph group) in the Ribbon.

Other formatting choices, such as hyperlinks or special symbols, can still be added to Word documents as needed.



Plateau PC Users Group, Inc.

Application for Membership for 2026-2027

----- New Member

----- Renewing Member

Return this application with a check for annual dues payable to "PLATEAU PC USERS GROUP"
Return to the club Treasurer during our meeting or mail to
"PPCUG Treasurer. 221 Tomlon Road, Crossville TN 38555"

Our annual dues are now payable July 1st. of each fiscal year.

Persons// families joining during the fiscal year have dues payable as follows:

<u>Join In</u>	<u>July - Sept</u>	<u>Oct - Dec</u>	<u>Jan - Mar</u>	<u>Apr - June</u>
Single	\$24	\$18	\$12	\$6
Family	\$30	\$22	\$15	\$7

Date: _____ Amount Paid: \$ _____ by Cash _____, or Check (# _____)

Last Name *First Name* *Family Member (if family membership)*

Address:

City *State* *Zip Code* (*Phone Number*)

E-Mail address: -----
Please Print

I have belonged to a Computer Club before: Yes _____ No _____

I have used PC's since (year): _____

I have knowledge in the following areas that I would be willing to share with club members:



November 2026



<u>Sun</u>	<u>Mon</u>	<u>Tue</u>	<u>Wed</u>	<u>Thu</u>	<u>Fri</u>	<u>Sat</u>
1 	2	3 	4 10:00 A.M. PPCUG Board Mtg.	5	6	7
8	9	10 3:00 P.M. General Mtg. Presentation. Followed by Q&A Session	11 	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26 	27	28
29	30					