Microsoft - Technology Support for our Older Adults Community

Microsoft 2022

Microsoft -Technology Support for our Older Adults Community

***Microsoft's mission** is to enable every person and every organization on the planet to achieve more.*

There are no limits to what people can achieve when technology reflects the diversity of everyone.

This playbook brings together the wide range of solutions available from Microsoft to support users with technology accessibility requirements.

https://www.microsoft.com/en-us/accessibility/

INTRODUCTION

In Microsoft, our aim is to create resources that will provide global support solutions for the elderly communities. By partnering with local non-profits, we aim to enable older adults with technology so that this community and its extended impact can feel included and connected in a safe, independent, confident, and empowered manner. Through new technical skills, senior citizens will solve problems and continue to participate in the ever-changing society.

This playbook showcases useful information and guidance about accessibility features relevant for the older adult's community, based on internal and market research shown in this age group. We aim the playbook to provide global support solutions to enable the older adults in our families, communities and customer base feel happier, more connected, independent & less fearful of using technology. It will enable them to learn technical skills and solve problems specific to their local needs whilst also educating them on using accessibility options to make it easier to interact with their personal computer and take part in society.

How to use this playbook:
This document includes a selection of key features and functionalities provided by Microsoft across our different technologies and products to enable and support a wide range of accessibility needs (vision, hearing, mobility). It also includes bits of useful information about Microsoft accounts and how to protect it as well as how to navigate the internet safely and how to protect your personal data. We've included after each section links to many useful online resources provided by Microsoft.

Content:

FOR VISION

Need a larger screen? A brighter screen? A narrator to read text? Find out about our accessibility tools and features for people who are blind, colour blind or have low vision

Distinguish colors easily

Boost contrast or get rid of color entirely—whether you have colorblindness, light sensitivity, or a visual preference, with color filters you can customize your screen's color palette.

Find out more by clicking **HERE**

Get a closer look

Enlarge words and images with Magnifier. And with the customized settings you can use it on all or part of the screen—whatever way suits you best.

Find out more by clicking **HERE**

Know where you are

Make your **mouse** as big or small as you want or make it black if that's best for you. Windows 10 offers many ways to customize your **mouse** and cursor size

Find out more by clicking **HERE** & read the section called **Know where you're pointing**

FOR VISION

Type what you want to do

Tell Me lets you quickly access commands in several Office 365 applications without navigating the command ribbon. You can use **Tell Me** to assist with formatting, discover the difficult-to-find capabilities and even get scoped help in Office 365 using everyday language

Find out more by clicking **HERE**

See every detail

Increase the colour contrast of text and images on your screen, making them easier to identify. Each high contrast theme can be customized to suit your needs and tastes.

Find out more by clicking **HERE**

Narrator

Narrator is the built-in screen reader in Windows that reads aloud what's on your screen so you can use that information to navigate your PC. To start or stop Narrator, press the **Windows logo key + Ctrl + Enter.**

For more info on how to use Narrator, check out the **Complete guide to Narrator.**

FOR HEARING

READ AND ENJOY

Use **closed captions** to read the words that are spoken in movies and television shows. With Windows 11 you can adjust the colour, size, and background transparency to fit your specific needs.

Find out more by clicking **HERE**

DON'T MISS A NOTIFICATION

Adjust notifications to make them appear on your screen longer. If you have difficulty seeing or hearing—or just prefer a longer alert—you can increase the alert display time up to five minutes

Find out more by clicking **HERE** and read the section called **Make Notifications stick around longer**

Getting Support

Customers seeking support for more complex issues in sign language can contact the Microsoft Disability Answer Desk through aka.ms/dad. Currently only supports American Sign Language, US.

About Your Microsoft Account

If you use any of these services, you should already have a Microsoft account: Outlook.com, Office, Skype, OneDrive, Xbox Live, Bing, Microsoft Store, Windows, or MSN. Your Microsoft account lets you manage everything all in one place. You manage your Microsoft account from the Microsoft account dashboard.

Sign in to your Microsoft account dashboard:

1. Go to Microsoft account and select Sign in.
2. Type the email, phone number, or Skype sign-in that you use for other services (Outlook, Office, etc.), then select Next. If you don't have a Microsoft account, you can select No account? Create one!. Note that we recommend using an email you already have and use regularly.
3. Type your password and select the Keep me signed in box if you want to go straight into your account next time (not recommended for shared computers).
4. Select Sign in.

If you forgot your Microsoft account email address or you signed in and got the error message, That Microsoft account does not exist, we recommend following the steps:

- Lookup your username if you have security info set up on your account
    1. Look up your username using your security contact phone number or email address.
    2. Request a security code to be sent to the phone number or email you used.
    3. Enter the code and select Next.
    4. When you see the account you're looking for, select Sign in.
    5. Check products or services where you used your Microsoft account
- Your account might be closed or deleted - You might not be able to sign into your account because it's closed or deleted.
    - You closed your account. If you closed your Microsoft account, you have 60 days from that closure to sign in and reopen it. After those 60 days, your account and data expire.
    - Your account was closed because of inactivity. If you haven't signed in to your account for a long time, it might expire due to inactivity, according to the following schedule.

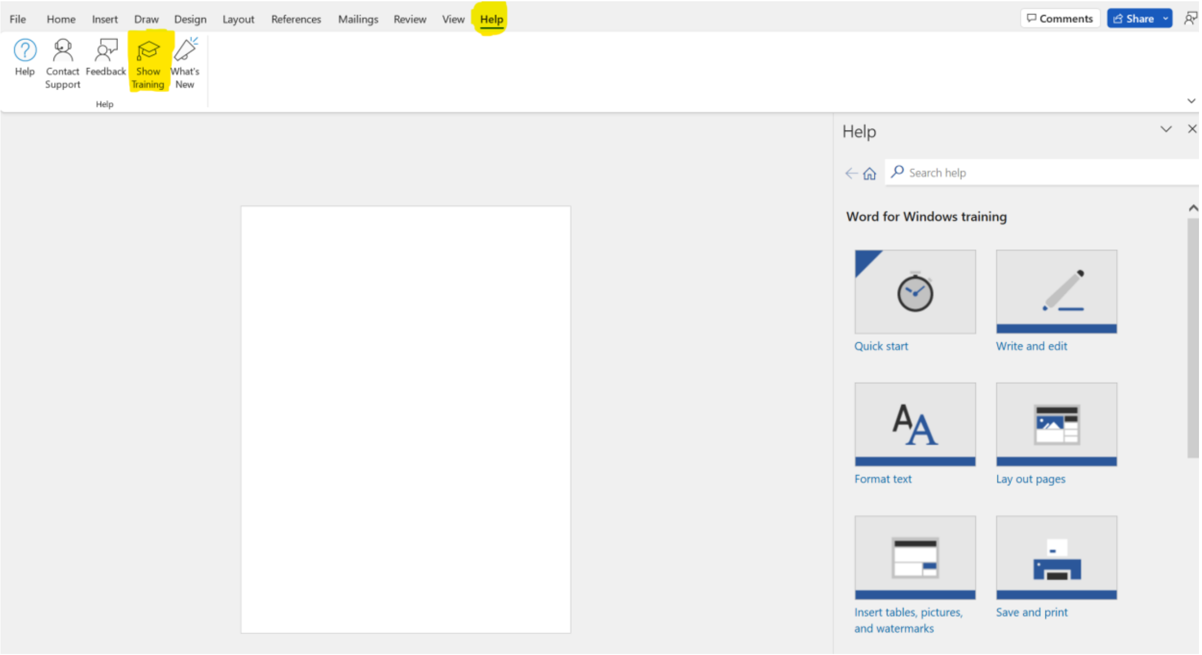
Find more information by clicking here.

Help resources for Office programs (1)

Microsoft offers a number of programs which you can use in your day to day life to manage your communication and activities. These include Microsoft Word, a word processing tool; Microsoft Excel, a spreadsheet program; Microsoft PowerPoint, used for creating interactive presentations; Microsoft Outlook, used for email and calendar management.

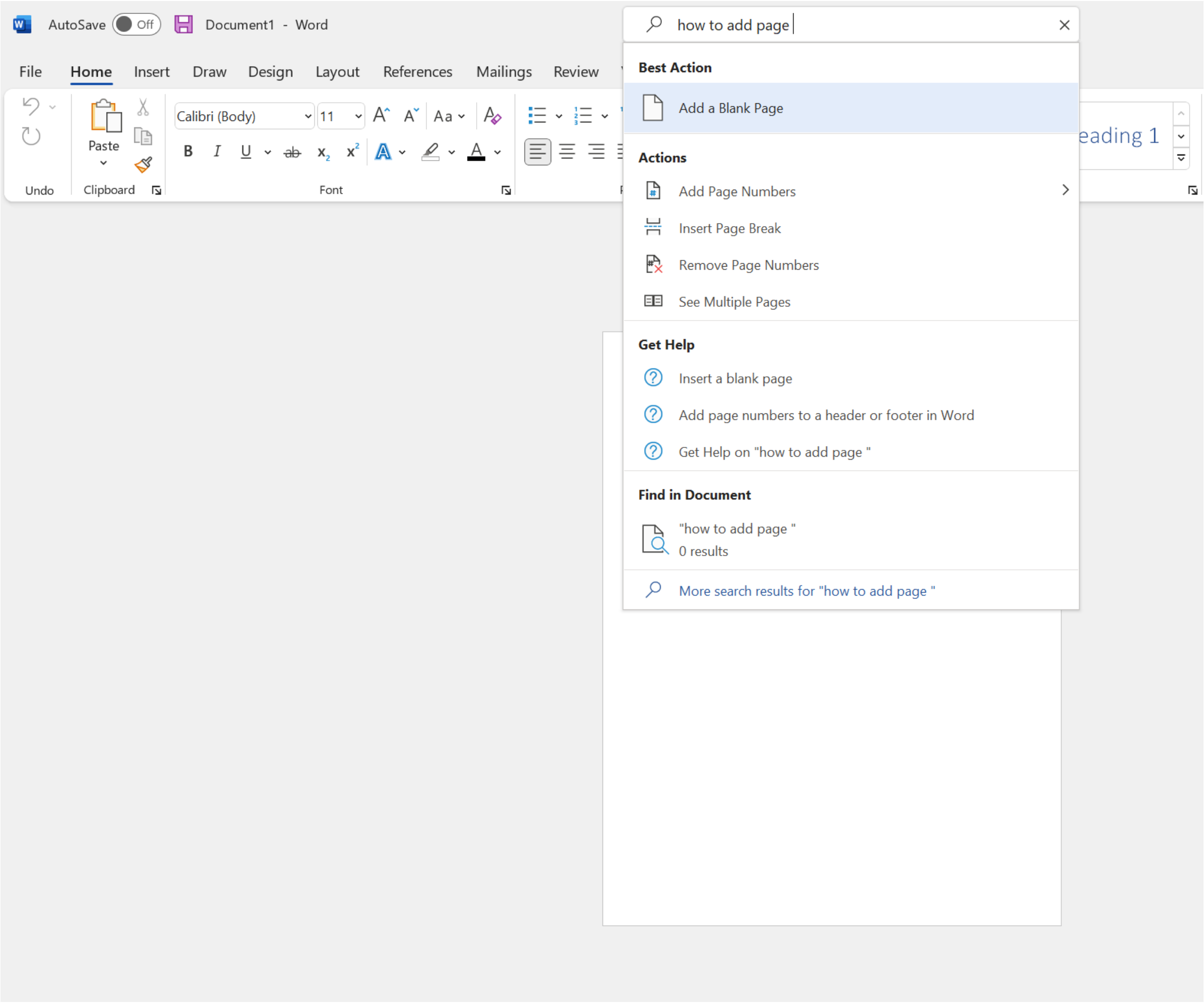
Each of these programs has a Help section where you can access information to help you use them with efficiency.

You can access the *Help* section as below, and from there access *Show Training*. This will give you access to a wide range of resources, video and text. These resources are also available in local language.



Help resources for Office programs (2)

Another way to learn how to use Office programs is to type your question in the Search section in the upper side of the page, as shown below:



how to add page

Online Safety

Your privacy on the internet depends on your ability to control both the amount of personal information that you provide and who has access to that information. When you read email, use social media, or browse the web, you should be wary of scams that try to steal your personal information (also known as identity theft), your money, or both. Many of these scams are known as "phishing scams" because they "fish" for your information.

Phishing is a popular form of cybercrime because of how effective it is. Cybercriminals have been successful using emails, text messages, direct messages on social media or in video games, to get people to respond with their personal information. The best defense is awareness and knowing what to look for. Here are some ways to recognize a phishing email:

- Urgent call to action or threats - Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams.
- First time or infrequent senders - While it's not unusual to receive an email from someone for the first time, this can be a sign of phishing. When you get an email from somebody you don't recognize, or that Outlook identifies as a new sender, take a moment to examine it extra carefully before you proceed.
- Spelling and bad grammar - If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.
- Generic greetings - An organization that works with you should know your name and these days it's easy to personalize an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.
- Mismatched email domains - If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam.
- Suspicious links or unexpected attachments - If you suspect that an email message is a scam, don't open any links or attachments that you see. Instead, hover your mouse over, but don't click, the link to see if the address matches the link that was typed in the message.

Find out more by clicking here

Online Safety

What is identity theft?

- When a thief gathers information about you and uses it to impersonate or defraud you, it’s called identity theft. Even a small amount of data—your Social Security number, password, address, mother’s maiden name, account number or PIN—is enough for a thief to make credit card purchases, open bank accounts, take out loans, or commit crimes in your name.

Four simple ways to help protect your identity online:

1. Be defensive with sensitive information

- Don’t put sensitive information in email, instant, or text messages. These methods may not be secure.
- Look for signs that a webpage is secure and legitimate. Before you enter sensitive data, check to ensure the web address starts with https (“s” stands for secure) and shows a closed padlock. (The lock might also be in the lower right corner of the window.)

2. Create strong passwords and keep them secret

- Strong passwords are long (phrases or sentences) that mix capital and lowercase letters, numbers, and symbols. Ideally your passwords should be at least 14 characters long
- Don’t use the same password everywhere. If it’s stolen, all the information the password protects, in all the accounts it's used on, is at risk
- Don’t share your passwords
- Writing them down is ok, as long as it's on a well-protected piece of paper away from your computer.

3. Protect your accounts and your credit

- Stay on top of existing account balances by reconciling account activity regularly.
- Report discrepancies quickly. The law protects you from having to pay for fraudulent transactions on your account, but only if you report them promptly.

4. Boost your computer’s security

- Reduce your risk of identity theft by keeping all software (including your web browser) current with automatic updating.
- Install legitimate antivirus and antispyware software. Windows 10 comes with Microsoft Defender Antivirus already installed and turned on.

Find out more by clicking here.

Online Safety

Keep your computer or tablet secure helps you avoid malware and direct hacking attempts designed to steal your personal information.

Tips to protect your computer

- Use a firewall - Windows has a firewall already built in and automatically turned on.
- Keep all software up to date - Make sure to turn on automatic updates in Windows Update to keep Windows, Microsoft Office, and other Microsoft applications up to date. Turn on automatic updates for non-Microsoft software as well, especially browsers, Adobe Acrobat Reader, and other apps you regularly use.
- Use antivirus software and keep it current - If you run Windows you have Windows Security or Windows Defender Security Center already installed on your device.
- Make sure your passwords are well-chosen and protected
- Don’t open suspicious attachments or click unusual links in messages.
- Browse the web safely - Avoid visiting sites that offer potentially illicit content. Many of these sites install malware on the fly or offer downloads that contain malware. Use a modern browser like Microsoft Edge, which can help block malicious websites and prevent malicious code from running on your computer.
- Stay away from pirated material - Avoid streaming or downloading movies, music, books, or applications that do not come from trusted sources. They may contain malware.
- Don't use USBs or other external devices unless you own them - To avoid infection by malware and viruses, ensure that all external devices either belong to you or come from a reliable source.
- Find out more by clicking here.

How to manage cookies

- Cookies are small files that websites put on your PC to store info about your preferences. Cookies can improve your browsing experience by allowing sites to remember your preferences or by letting you avoid signing in each time you visit certain sites.
- However, some cookies may put your privacy at risk by tracking sites that you visit.
- Find out more about how to delete or block/allow cookies by clicking here.

Online Banking

When it comes to your online banking activity, each bank and banking service will have its own processes and regulations. We recommend you remember the information provided in the Online Safety section of this playbook and keep in mind:

- Don't click or open emails or file attachments that seem suspicious. If these seem to come from your bank, check for spelling or bad grammar, generic greetings or mismatched email domains.
- Never offer information such as your bank card number, passwords or personal information via phone or email
- Reach out to the customer service line of your bank or visit your local bank directly if possible to verify what kind of information they need from you
- Most banks and banking systems have online applications that you can use to make payments safely. Ask your bank about their official application and set up an account so that you can use your information under protection. You can use your personal email address and a password of your choice and remember the guidance included in this playbook under the Microsoft Account section (use a strong password)

Support And Accessibility Resources

- Accessibility features on Windows 11
- Microsoft Accessibility Features
- What is a Microsoft account? | Simply Windows - YouTube (2 min)
- What is a Microsoft account? | Microsoft - YouTube (1:18)
- What to do if you can't sign in to your Microsoft account | Account recovery | Microsoft - YouTube (2:36)
- How to unlock a suspended Microsoft account | Microsoft - YouTube (1:30)