Microsoft

Confidence to move forward

Purchasing software can be quite tricky as counterfeit products and services exist in the market. Avoid the risk, help stay safe, and purchase Genuine Software.

Today, business leaders and organizations are already looking for the opportunities to rebound, rebuild and thrive in the new normal. Microsoft supports its partners and customers with genuine software that offers better security, greater productivity, and support to help them move forward with confidence.

Confidence to always deliver on our promises. Confidence to help keep our customer data safe and reputations intact, so their businesses continue to run smoothly and grow securely. Confidence to help our people get more done from anywhere. And confidence to be the best business partner.

Help your business with genuine Windows and Office, and follow the trail of 'confidence to move forward'.

66%
of end-users have problems with software obtained from suspect sources

33%
chance of malware if PC has unlicensed software

24%
of malicious programs in pirated software can deactivate anti-malware solutions

Unlicensed software poses a number of risks

Think twice before you acquire a software. Unlicensed software may have viruses and would not have sufficient security measures, which would leave the door open for hackers and viruses.

- Your **identity can be compromised** and used for financial gains and criminal activities.
- Hackers can clone your credit card and access bank resulting in **financial loss**.
- You can **lose important personal files and business data** like customer & accounting information.
- Your business **operation can stop**.
- You may become **vulnerable to malware attacks**.

Top four cyber threats in India

Malware
Malware poses risks in the form of impaired usability, data loss, intellectual property theft, monetary loss, and even emotional distress.

Cryptocurrency mining
Attackers seeking illicit profits have increasingly turned to malware that lets them use victim's computer to help them mine cryptocurrency coins.

Ransomware
While individuals and organizations are becoming more intelligent in dealing with ransomware, it continues to be a significant threat in India.

Drive-by download
Attackers are exploiting vulnerabilities in webpages to direct users to compromised sites that can secretly infect users even when they do not attempt to download anything.

Source

- https://www.microsoft.com/mea/genuine/#gsc-risk-number
- https://www.microsoft.com/mea/genuine/how-to-tell.aspx
- https://news.microsoft.com/uploads/2017/10/Whitepaper-Cybersecurity-Risks-from-Non-Genuine-Software.pdf

Have confidence to move forward

with genuine Windows and Office

Microsoft genuine software helps provide the security, updates, and support that businesses need. It brings in complete protection from Day 1 via Microsoft Defender Antivirus with its latest and up-to-date antivirus, as well as phishing, ransomware, and malware protection technology.

The best part about Microsoft genuine software is that it comes with automatic and hassle-free updates that are free and for the lifetime of your device. And there is free set-up support from Microsoft along with 24/7 help by phone, live chat, and support resources.

Identifying a genuine Microsoft software

Watch out for the 3Ps

Product packaging

A genuine product will never have spelling errors, blurry text, or incorrect logo. The Certificates of Authenticity (COA) label is used on the outside of retail boxed software and explains what the product is, its country of intended use and country of origin.

Product's authenticity

Avoid auction sites and Peer-to-Peer file-sharing sites. At the moment, there are a limited number of sites where you can legally purchase digital downloads of Microsoft software and one such example is the official Microsoft Store.

Product label

A genuine Microsoft Software will always have a Certificate of Authenticity label, embedded hologram, and a 25-character unique product key.

YouTube

In India, Microsoft has deployed a unique authentication label on fully packaged product (FPP). The label can be found next to the retail box COA.

Tips for safer shopping — in person or online

Buying online can be quick, convenient and a great value; however, it does not always give you the same opportunity to see exactly what you are getting as walking into a regular store. The general rule to remember is that if the price looks too good to be true, it probably is.

Make sure you are getting what you paid for

Buy from a reseller you trust. Ask the person or business, specific questions about key features of the item you are interested in buying.

Get the right software

Make sure to determine whether the software you are buying is intended for home use or for business use.

Shopping online?

Use a secure payment method. Do not pay with cash or with instant money transfers.

Beware of Product Keys sold separately

Apart from Product Key Cards (PKCs) distributed with COAs, Microsoft does not distribute products keys as standalone products.

Report a counterfeit software

You may file an online report on Microsoft's site if you inadvertently bought or received counterfeit software.

Protected software buying guide

Buy from trusted sources

When purchasing software, make sure it's from a credible source. A trusted reseller or the Microsoft Store are your go-to options.

Use only licensed software

Always make sure the software is properly licensed - whether it's Windows or Office.

Verify product key source

For digital downloads, make sure the product key comes from a trusted source and not from an instant messaging platform or email.

Avoid discount and sale offers

Don't fall into the trap of discounts and cheaper software packages. You may end up paying much more in recovering lost data or legal damages.

Check for brand packaging

Make sure the packaging of the physical product includes an authentic Microsoft logo and brand identity. Be wary of standalone stickers or product key cards, they don't grant the right to use Microsoft software.

Accept only sealed packages

The package of the physical product must be sealed to ensure first time use. Product keys are designed to work on a single or limited number of devices.

Check for updates

Regularly updating your software helps protect you from potential hackers and viruses.

Make security a collaborative journey

The Zero Trust security model is no longer a business option but is an imperative. Based on the principle of "never trust, always verify," the security posture treats each step across the network and each request to access for resources as a unique risk to be evaluated and verified.

While organizations put in place necessary access and preventive controls, use cloud storage services to automatically backup important data, leverage cloud technology to limit attackers' access to data and help security operations respond better to attacks, employees should also be educated on safe cyber practices. Employees should know how to spot phishing and social engineering attacks and practice credential hygiene.

Counterfeit software: Are you using it without even knowing it?

Scan this QR code to learn how to identify a genuine software

Or visit: www.aka/ms/onlygenuine

Learn how to tell whether your Microsoft software and hardware are genuine, by visiting: https://aka.ms/howtotell

For more information about genuine software, visit http://aka.ms/onlygenuine.