Microsoft

Counterfeit software – It's simply not worth the risks.

There are real risks associated with counterfeit software. Be aware of these risks and the importance of always providing customers with the genuine software they expect and deserve.

Viruses, malware, Identity theft.

1 in 3 consumer PCs with counterfeit software installed will be infected with malware*. That puts these users at increased risk for identity and bank account theft, and also increases the chance they'll pass on a virus to colleagues or friends.

Damage to PCs and devices.

Counterfeit software can have disastrous effects on the performance of your customer's PCs and devices – both at work and at home. Ensure your customer's technology investments aren't exposed to these risks.

A good deal gone bad.

Fixing the serious issues caused by counterfeit has consequences that are both time-consuming and expensive. Any software cost savings realized by purchasing counterfeit is quickly reversed when fixing the damages. It simply isn't worth it.

Damage to your reputation.

Your reputation means everything. Your business depends on it for delivering reliable products and services. Counterfeit software distribution can damage your reputation as well as customer trust and loyalty.

Help both your business and consumer customers understand the specific risks counterfeit software poses to their demographic.

Professionals

Using counterfeit software can expose you and your company to harmful malware or viruses. This can lead to loss of sensitive information, unauthorized access to confidential company information, and infection to others across your network.

Parents

Using counterfeit software can expose all PCs and devices in your home to criminals who want access to your confidential information. It can put your family at increased risk for identity and bank account theft.

Students

Using counterfeit software can spread dangerous viruses and malware to all your friends and social media contacts. It can cause PC crashes and loss of data.

Types of Piracy

Make sure you understand the different types of piracy and how to ensure your customers are getting only genuine software. Remember that if the price looks too good to be true, it probably is.

Piracy Type	Definition	How to Avoid
Hard Disk Loading (installation piracy)	Hard disk loading (installation piracy) occurs when a system builder installs (and typically activates) one license onto **multiple** devices, then sells the devices without accompanying software licenses. The system builder avoids the license costs, but typically charges the customer for the illegitimate software. Customers may remain unaware of any pirating until they encounter issues.	Ensure you are providing your customers with a genuine, fully licensed version of software to accompany software you have installed on a new PC. Microsoft OEM Software is designed specifically for this purpose, and can be purchased from Microsoft Authorized OEM Distributors. Learn more at **http://aka.ms.msoemwindowslicensing** and **http://aka.ms.msoemdisti**.
Online Downloads	Software distributed illegally via peer-to-peer networks or downloaded through unauthorized sites. This software often contains harmful malware and viruses that can put users at risk.	Only download Microsoft software from sites you know are legitimate, such as the Microsoft Store. Never download from any peer-to-peer networks, BitTorrent index sites, or one-click file hosting sites. Learn more at **http://aka.ms/mssoftwaredigital** **www.bsa.org/anti-piracy/internetpiracy**.
Standalone Certificates of Authenticity (COAs)	Standalone COAs are COAs that are sold by themselves, without the accompanying software they authenticate. They are often branded as "excess inventory" or "unused labels" and are often counterfeit versions of COAs. Purchasing standalone COAs and passing them off to unsuspecting customers is a form of piracy.	COAs should never be sold, shipped, or purchased on their own, without being affixed to a PC or sold with related Microsoft software (either full packaged product or Microsoft OEM software acquired by system builders). Do not fall victim to standalone COAs. Learn more at **http://aka.ms/mshardwarepcpurchase**.
Leaked Volume License Keys (VLKs)	Microsoft Volume Licensing Agreements for large organizations provide Volume License Keys (VLKs) for Microsoft product activation in certain scenarios. The unauthorized distribution of these VLKs, outside of the organization to which they are tied, is a form of piracy.	Only those devices that are a part of the organization with the Volume Licensing Agreement may use their assigned VLKs. VLKs are never legitimate when sold or distributed outside of the organization to which they are tied. Never purchase or illegally use or download a VLK. To learn more about VLKs visit: **http://aka.ms/mslicensingfaqproductactivation**.
Online Auction Sites	Pirated or unauthorized software is often distributed via online auction sites, where sellers take advantage of unsuspecting buyers. Sellers may be offering second-hand product, previously activated product, stolen or used COAs, illegally copied DVDs, etc. Buyers are often left without recourse once they discover they have been a victim of piracy.	Be careful when buying from online auction sites. Ask important questions. Does the software come in its original packaging? Does it include all necessary components? Is the price too good to be true? Is it being sold by a reseller you know and trust? Learn more at **http://aka.ms/msonlineshopping**.

*International Data Corporation, DANGERS OF COUNTERFEIT SOFTWARE STUDY 2013