Cyber security, daily use

2648 Nov 12, 2024 Other

To increase the security of your computer, we've listed a number of best practices. This article shares a few tips for everyday computer use.

Private use

If you also use your work computer for private purposes, create a separate user account for private use. This way you will avoid mixing your private and professional email accounts and documents.

Session lock

If you use your computer in an unsecured setting (outside your office or home), prevent unauthorized people from using your computer without your knowledge. Set your session lock to a few minutes of inactivity and to immediately when the computer goes to sleep.

USB sticks / external hard drives

USB sticks and external hard drives are convenient for transferring files between computers. However, malware takes advantage of them as a transmission vector to infect new computers. Therefore, the use of USB sticks and external "nomadic" hard drives should be avoided whenever possible. Instead, use online services such as Swisstransfer to transfer files.

File sharing services

In the same logic as USB sticks, file sharing services such as Dropbox, Google Drive, Microsoft Drive, kDrive can be used by "malware" to spread. Use them sparingly and avoid sharing dedicated disk space with people outside your company as much as possible.

Up-to-date software versions

Never install pirated software or software obtained from anywhere other than the official software site. Software on illegal sharing sites is frequently compromised.

When a new version of a software or operating system (Windows or macOS) is released, do not delay in installing it. Indeed, old versions of software often have known security flaws that can be exploited by criminals.

In case of a major update, make sure beforehand that it is compatible with your production environment (software, computer, printers...). And avoid installing beta versions (not finalized) on your computers in production, at the risk of losing time with dysfunctions.

In case of infection

If malware has entered your computer, unusual behavior may occur that alerts you. Report your suspicions to your IT manager immediately and prevent the malware from spreading by disconnecting your computer from the network. However, avoid turning off your computer in

order to let the specialists examine it.

Online URL: https://om-bm.knowledgebase.co/article-2648.html