Two types of malware known as exploits and Zero-day attacks refer to cybercriminals taking advantage of vulnerabilities in the software products we use every day. These include operating systems like Windows, web browsers like Chrome, Internet Explorer and Firefox, and a wide range of popular applications like Adobe Flash and Reader, Java and Skype.

Malware writers invest a lot of time and energy searching for faulty software code they can exploit and use as a backdoor into your PC to deliver malware for any number of malicious purposes. Zero-day attacks are named as they are because at the time of their discovery there is no fix for the vulnerability they are exploiting, leaving software companies scrambling to release updates within a few days, which is plenty of time for cybercriminals to spread malware.

Tip: The best defense against malware exploits is to always update software programs to the latest available versions. When a message appears on your screen to update a trusted software application, do it. Chances are good the software developer is correcting an issue that may have serious security implications. We use Kaseya, as an automated patching solution, so these updates should be deployed automatically. However, be mindful of Zero-day alerts from MIS, which may instruct you to avoid using certain programs when a threat is identified.