UNDERSTANDING FILE TYPES

With design, videography, photography, and web there are many file types out there. Without certain software, specific file types cannot even be opened by the average person. It is important to understand the differences between them though, so that you can use them properly and get the best quality out of each. Below is a list of the most common file types, what they are, and what they are used for.

Popular File formats

1. JPEG file is a compressed image file that does not support a transparent background. The level of compression in JPG files can vary in resolution with high quality for desktop printing, medium quality for web viewing and low quality for email.

2. PNG files stand for Portable Network Graphics. This format has built-in transparency, but can also display higher color depths than JPEG, which means higher resolution.

3. EPS files are most commonly used by designers to transfer an image or artwork, generally a vector file into another application. Vector-based EPS files are scalable to any size. EPS files can be opened using Adobe Illustrator, Freehand, or Adobe Photoshop.

4. GIF is a widely used web image format, typically for animated graphics like banner ads, email images and social media memes. They can be exported in a number of highly customizable settings, which in turn reduces the file size.

5. PDF is a universal file format that preserves/embeds all elements of any source document (holding its design). PDF files can be shared, viewed and printed by anyone with the free Adobe Reader software.

[REDACTED]

Standardized file formats play a key role in the development and use of computer software. However, it is possible to abuse standardized file formats by creating a file that is valid in multiple file formats. The resulting **[REDACTED]** (many languages) file can confound file format identification, allowing elements of the file to evade analysis. This is especially problematic for malware detection systems that rely on file format identification for feature extraction. File format identification processes that depend on file signatures can be easily evaded thanks to flexibility in the format specifications of certain file formats. Although work has been done to identify file formats using more comprehensive methods than file signatures, accurate identification of **[REDACTED]** files remains an open problem. Since malware detection systems routinely perform file format-specific feature extraction, **[REDACTED]** files need to be filtered out prior to ingestion by these systems. Otherwise, malicious content could pass through undetected.