

Best Practices Guide to Use of Digitized Signatures

October 4, 2006

Digitized images of handwritten signatures are appearing more and more frequently in electronic mail messages and other digital documents. These signatures are most often created by scanning one's signature into an image file. Including such signature files in widely distributed electronic documents increases the risk that they may be fraudulently used by others.

IT Security recommends the following best practices in the use of such digitized signature files.

1. Recognize that your signature (i.e., the one you use to sign checks and other legal documents) is personally identifiable information. In the wrong hands, it can prove just as damaging to you as disclosure of your social security or driver license numbers.
2. Avoid creating or storing a digitized version of your signature in any format unless there is a true need to do so. If your computer is ever compromised, this file could be stolen and assist in the theft of your identity.
3. If you wish to give your name a more personalized appearance in an electronic document, consider using one of the many available script fonts. Examples of these fonts include:

Freestyle Script

Brush Script MT

Edwardian Script.

Lucida Handwriting

Vladimir Script

Questions regarding this message should be directed to IT Security at ITSecurity@txstate.edu or 512-245-HACK.