Forgery (2): Desktop Forgery

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Forgers have gone high-tech. It seems nothing is sacred any more, not even certificates and signatures.

High-quality color scanners, a PC with good image-enhancement (touch-up) programs and high-resolution color printers have made forgery a snap. Even before modern image-processing technology was available, forgers knew that the appearance of a document cannot guarantee its origin once there are ways of imitating that appearance.

There have been many examples of computer-related forgeries. For example,

* A Boston resident forged checks by digitizing company logos and printing them on check stock. He defrauded computer suppliers and sold stolen computers all over the Caribbean. Another forger generated official-looking documents from the Connecticut Bank & Trust company attesting to his financial reliability. Using these references, he is alleged to have borrowed more than $10 million and then filed for bankruptcy after moving the money offshore.

* A European thief deposited and then withdrew $3 million in fake cashier's checks made with a laser printer and a color copier.

* Prisoners have managed to effect their own release by sending a FAX of a forged document to their prison officers.

* California State Police in Los Angeles once arrested 32 people for issuing fake smog control certificates. Each certificate sold for about $50.

* Another forgery case involved the CIA--as victims, not perpetrators (for a change). In October 1992, Joseph P. Romello pleaded guilty to having defrauded the CIA of more than $1.2 million. In one of his crimes, he tricked the Agency into paying $708,000 for nonexistent computer hardware and provided forged documents for the files showing that the equipment had been received.

* * *

Some practical suggestions:

At your place of work, be sure that everyone understands that it is illegal in the USA to make copies of currency. Title 18, section 471 of the US Code provides for jail terms up to 15 years for having counterfeit bills or for altering currency to increase its apparent value. And “It was just a joke” is unlikely to be a successful excuse.

You should verify the authenticity of documents before acting on them. For example, if a candidate gives you a letter of reference from a former employer, verify independently that the
phone numbers match published information; call the person who ostensibly wrote the letter; and read them the important parts of their letter.

Don’t trust signatures blindly: a good scanner and a color printer can reproduce anybody’s signature and make it appear to have been signed with a pen. Detecting a real signature can involve microscopic examination to measure indentations in the paper that are created by a real pen but not by a printer.

Financial institutions should be especially careful not to sign over money quickly merely because a paper document looks good. Thorough verification makes sense in these days of easy forgery.

* * *

For more about counterfeit money, see <http://www.bep.treas.gov/document.cfm/18/103>

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.