Beware of get-rich-quick schemes on your e-mail

Hanford employees have again reported receiving unsolicited requests via e-mail, letter and facsimile from individuals claiming to be official representatives of various overseas government offices. The requests typically ask for support in moving large sums of money out of the country, and offer the victim a substantial reward for assisting in the transfer of funds.

The U.S. Secret Service currently refers to these as “4-1-9” or “Advance Fee Fraud” schemes. The term “419” refers to the Nigerian criminal statute for fraud where many of these e-mails originate.

Beware; these requests for funds are part of a long-standing scam that has the following characteristics:

• The financial solicitation letters have largely originated from the country of Nigeria, but a growing number are originating elsewhere.

• Although the letters have been written in various contexts and have originated from varying individuals with official-sounding titles, the messages are all essentially the same. The authors are attempting to obtain American bank accounts for depositing large funds as part of closing a business transaction.

Practicing Operations Security, or OPSEC, at home can help minimize vulnerabilities to your personal information. For example: never divulge your bank-account numbers, credit-card accounts, or other sensitive information to people unknown to you. Con artists from the United States like to use the telephone, but their use of e-mail is growing. You can prevent your trash from becoming someone’s treasure by shredding personal information, such as pre-approved credit cards, credit-card receipts, paycheck stubs, items bearing Social Security numbers, banking information, medical records and investment data. ■

• The letters claim that if you wish to participate in the business dealings and provide your bank-account information, you will receive a hefty percentage of the millions of dollars to be gained simply because of your assistance.

• In some cases, the letters will attempt to get you to travel to Nigeria or another third-world country, where you can be blackmailed or additional funds extorted from you. There have been several reported cases of violence against victims, including murder.

• In some cases, the scenario appears to be totally risk-free at first, implying that no money needs to be fronted by the intended victim at all. The con artists only want to initiate contact so they can draw the unsuspecting victims further into the scam before ultimately swindling them out of money.

The Federal Bureau of Investigation advises that there are known con artists operating out of Nigeria who are attempting to drain the financial assets of anyone willing to cooperate.

If you receive one of these letters, either via e-mail or through regular mail or fax, *Do not* attempt to contact these individuals. Because of the large number of mass mailings, Security is no longer asking that these messages be forwarded to them. Simply delete the message and remind yourself that if the message seems too good to be true, it probably is. ■