

THE CREDIT UNION JOURNAL

www.cujournal.com THE NATION'S LEADING INDEPENDENT CREDIT UNION NEWSWEEKLY April 24, 2006

By Kevin Jepson, *Technology Correspondent*

FT. WORTH, Texas—E-mail isn't private, but apparently millions of credit union employees and members are using it freely to send account numbers, passwords and loan information across the open lines of the Internet.

E-mail abuse was so bad at \$570-million EECU in Ft. Worth, Texas, that CIO Bill Burrows launched an automated e-mail encryption platform to protect members' information. "The problem was far more urgent and widespread than I thought," explained Burrows.

Despite warnings to members about sending private information over the Internet, EECU found that nearly half of the incoming e-mails to the Member Services Center contained an account number or other personal information, Burrows said.

"That was the first surprise," he continued. "To make matters worse, I also found that Member Services, collections, lending, real estate and accounting were all sending and receiving e-mails that really should have been encrypted."

EECU's scenario repeats itself at many credit unions, yet few CUs seem to encrypt their e-mails, according to early adopters such as EECU, the \$310-million Air Academy FCU in Colorado Springs, Colo., and the \$32-million TPS CU in Toledo, Ohio.

"To be generous, I would guess that less than half of all credit unions in the country are encrypting their e-mails," Burrows said.

E-mail encryption makes good sense. In addition, Gramm-Leach-Bliley Act and the NCUA effectively mandate it. "At the very least, I would think that the reputation risk to the credit union would be huge, even monumentally criminal, if sensitive information was intercepted by the wrong people," said Bob Tracy, CEO at TPS CU.

In light of the innumerable 'what-if' scenarios, credit unions have "two choices: wait until e-mail identity theft and fraud happens and clean it up later, or try to prevent it now," said Tim Grove, systems analyst at EECU.

EECU went with the second choice, launching the Tumbleweed MailGate e-mail compliance, security and anti-spam solution in December.

TPS CU followed suit last month, protecting messages with the SecureWorks Encrypted E-mail service.

Now, both credit unions' incoming and outgoing e-mails can be automatically encrypted, based on the credit union's rules. Outgoing e-mail is encrypted if the automatic filter finds selected words or number patterns in the message. In addition, employees can choose to encrypt e-mail by typing special words or symbols into the subject field.

Members can also protect their e-mails by signing-in to the web-based encryption mailbox to view or compose. Whereas EECU and TPS CU are happy with their encryption solutions, EECU said that Tumbleweed ended up being the better deal.

"The hosted solutions from Zix, the SecureWorks Zix hosting solution and Tumbleweed all had about the same initial

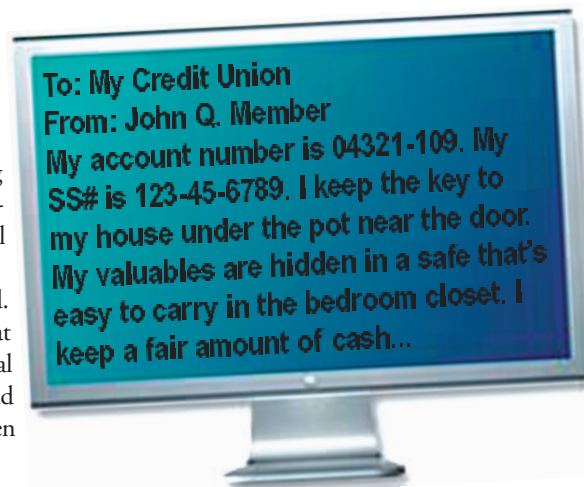
cost, but Tumbleweed was lower cost in years two and beyond," Burrows said.

Though Tumbleweed requires more internal support, it was "relatively easy to install, configure, and support," he said.

The e-mail filters do more than protect EECU against identity theft and fraud, Burrows added.

"On the first day we installed Tumbleweed, we found an e-mail in which one of our employees was sending a resume to another financial institution," he said. "Incidentally, the resume had factual errors."

e (ncrypting) -mail



Is Unencrypted E-Mail The Weak Link In Your CU's Security?

 Tumbleweed®

Tumbleweed Communications Corp. 700 Saginaw Drive, Redwood City, CA 94063
Tel: 650-216-2000/800-696-1978, Fax: 650-216-2001, www.tumbleweed.com