

it Index

18, 23, 31	Celent	25, 31
31	Citigroup	23
23	Clearing House Payments Co.	12
31	ColdSpark	29
26	Corillian	31
17	D	
17	Day Software	29
29	Deloitte Consulting	17
17	Deutsche Bank	32

Discover	14
----------	----

E-F

E*Trade	31
ECCHO	33
EDB Business Partner	17
EMC	29
Endpoint Exchange	33
Fair Isaac	17
Financial Insights	14
First Data	17
Fortis	26
FRS	17
FSTC	12
Fundtech	17

G-L

GainClients	32
Gartner	29
GE Capital	32
GMAC	32
Goldman Sachs	24, 29
HSBC	12
Intuit	18
Investars	24
JPMorgan Chase	12
Liquid Machines	29

M-O

MasterCard	14, 23
MessageGate	29
Metavante	22
National City	23
Norkom	26
NTT DoCoMo	12
Obopay	14
Oracle	29

P-S

PayPal	14
RSA	31
SAS	26
SVPCO	33

T-W

TowerGroup	26, 33
ViewPointe	33
Visa	14
VIVotech	14
Vuecentric	32
Wachovia	31
Wells Fargo	33

Letter to the Editor

To the Editor:

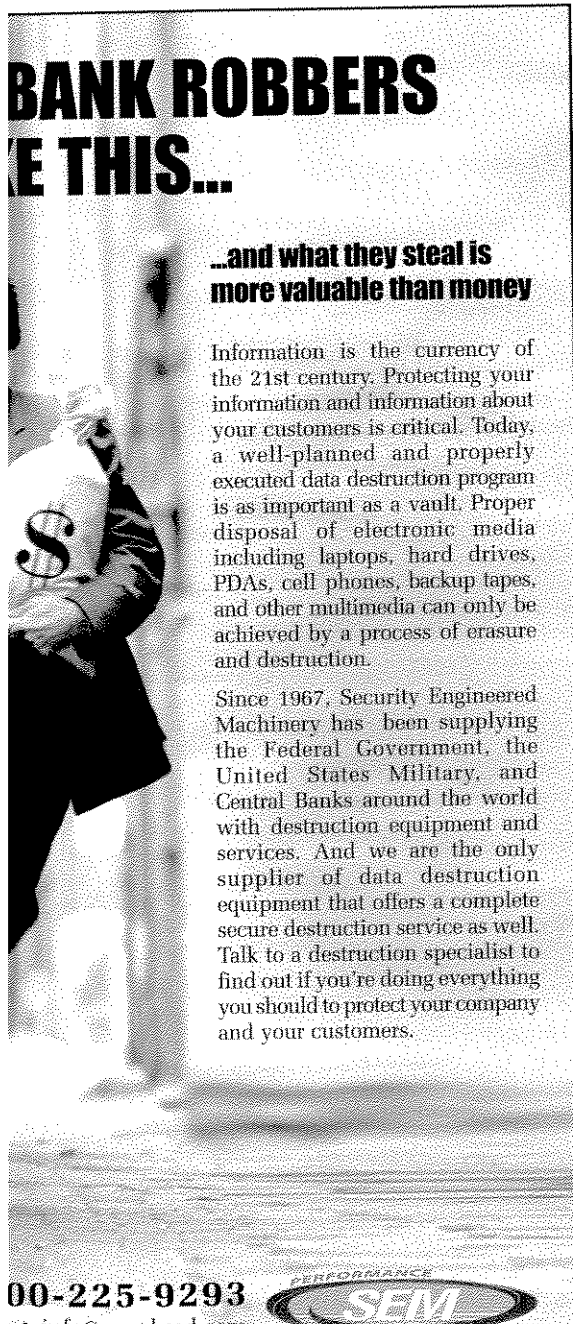
I read with interest John Adams' article, "Phishing Trip: A Magic Bullet Becomes the Crooks' New Weapon" (January). The article, which outlines recent phishing schemes that play on banks' movement toward multi-factor authentication, reveals some of the inherent weaknesses in the Federal Financial Institutions Examination Council's (FFIEC) dual authentication guidelines.

While dual-factor authentication is a step in the right direction, it has proven to be unsuccessful at thwarting man-in-the-middle attacks because the link between the user and their ISP can be hacked into and re-routed to a fraudulent site, thus compromising the security around the data being transferred. Dual authentication solutions that simply authenticate the site to the user, and not who the user really is, do not guarantee a trusted infrastructure.

To truly protect against fraud, multi-factor authentication must be performed across all levels, using a single, comprehensive solution that cross-authenticates the user to the site and the site to the user, and secures the two through digitally-issued, encrypted certificates that require a public and private key for access. Also critical are the ability to sign both the data and the container in which it is sent, as well as the capability to validate certificates against a real-time updated list that indicates whether or not the certificate has expired or been revoked.

A Public Key Infrastructure (PKI)-based approach, in conjunction with a second authentication method—such as hard or soft tokens—combines two strong authentication approaches, and provides the strongest authentication. Adding site validation on top of this ensures the most comprehensive approach to identity authentication.

Andrea Klein
Chief Marketing Officer
IdenTrust



BANK ROBBERS WANT THIS...

...and what they steal is more valuable than money

Information is the currency of the 21st century. Protecting your information and information about your customers is critical. Today, a well-planned and properly executed data destruction program is as important as a vault. Proper disposal of electronic media including laptops, hard drives, PDAs, cell phones, backup tapes, and other multimedia can only be achieved by a process of erasure and destruction.

Since 1967, Security Engineered Machinery has been supplying the Federal Government, the United States Military, and Central Banks around the world with destruction equipment and services. And we are the only supplier of data destruction equipment that offers a complete secure destruction service as well. Talk to a destruction specialist to find out if you're doing everything you should to protect your company and your customers.

00-225-9293
info@semshred.com

