



Brian Krebs on Computer Security

### The New Face of Phishing

Phishing is a difficult enough form of fraud to avoid for most computer users, but when some of the biggest names in the financial industry fail to do their part to detect and eliminate these online scams, consumers often are placed in an untenable situation.

Case in point: A source recently forwarded a link to one of the "best" phishing attacks I've ever seen. This one -- targeting the tiny **Mountain America** credit union in Salt Lake City, Utah -- arrives in an HTML-based e-mail telling recipients that their Mountain America credit union card was automatically enrolled in the Verified by Visa program, a legitimate security program offered by Visa that is supposed to provide "reassurance that only you can use your Visa card online."



The fake MountainAmerica.net Web site

The e-mail includes the first five digits of the "enrolled card," but those five digits are found on all Mountain America bank cards, so that portion of the scam is likely to be highly convincing for some recipients. The message directs readers to click on a link and activate their new Verified by Visa membership.

Now here's where it gets really interesting. The phishing site, which is still up at the time of this writing, is protected by a Secure Sockets Layer (SSL) encryption certificate issued by a division of the credit reporting bureau **Equifax** that is now part of a company called **Geotrust**. SSL is a technology designed to ensure that sensitive information transmitted online cannot be read by a third-party who may have access to the data stream while it is being transmitted. All legitimate banking sites use them, but it's pretty rare to see them on fraudulent sites.

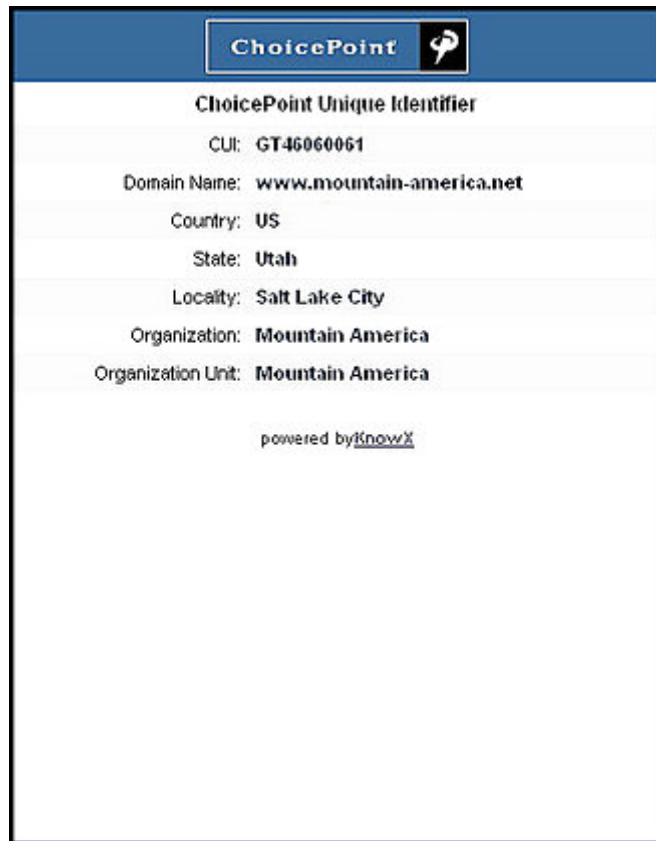


The SSL Certificate issued to Mountain-America.net

Geotrust and other SSL issuers are supposed to do some basic due diligence to ensure that the entity requesting an SSL certificate is indeed authorized to request it on the company's behalf. In this case, however, it looks like that process fundamentally broke down. Once a user is on the site, he can view more information about the site's security and authenticity by clicking on the padlock located in the browser's address field. Doing so, I was able to see that the certificate was issued by Equifax Secure Global eBusiness CA-1.

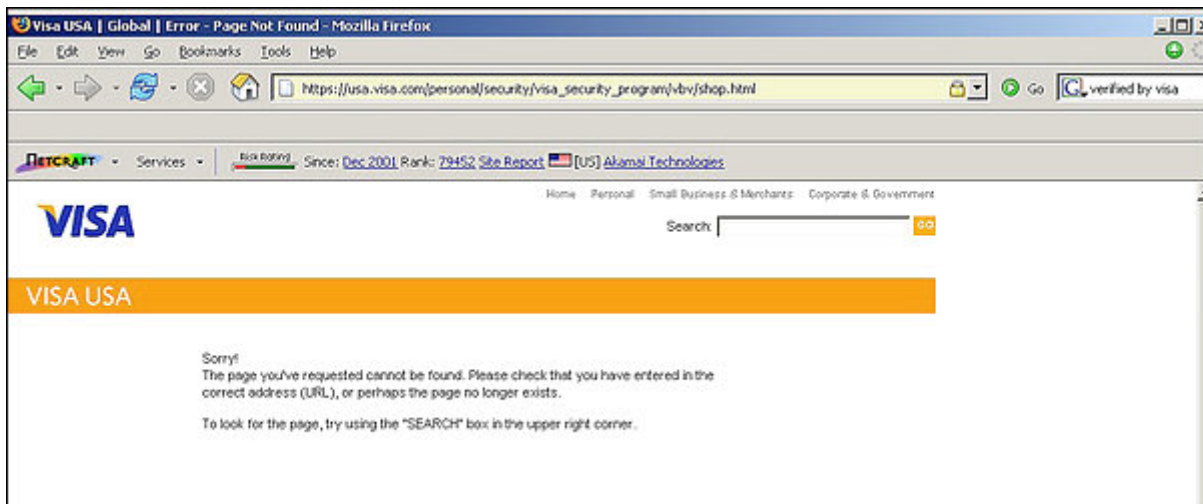
The certificate also contains a [link to a page displaying a "ChoicePoint Unique Identifier"](#) for more information on the issuee, which confirms that this certificate was issued to a company called Mountain America that is based in Salt Lake City (where the real Mountain America credit union is based.)

Choicepoint is a data aggregator that bills itself as "the nation's leading provider of identification and credential verification services." When Geotrust issues a certificate, Choicepoint provides a unique identifier -- an alphanumeric identifier that is supposed to be linked to a "corporate profile" that people can use to learn more about the recipient of that certificate. However, the profile page on this particular phishing site didn't have any more information than was already included in the rest of the certificate, including the company's name, city and state of incorporation, and the company's Web site (in this case, the profile refers to the phishing site's address.) It's unclear to me how the unique identifier adds anything that is of use to the person trying to verify the legitimacy of a Web site.



ChoicePoint's "Unique Global Business Record" for Mountain-America.net

I put a call in to the Geotrust folks. Ironically, a customer service representative said most of the company's managers are presently attending a security conference in Northern California put on by [RSA Security](#), the company that pretty much wrote the book on SSL security and whose encryption algorithms power the whole process. When I hear back from Geotrust, I'll update this post.



The error page generated by Visa.com

Back to the Verified by Visa program. Users who get the phishing e-mail described above -- or any genuine communications prompting them to visit the Visa site -- might think they're being sent to another fraudulent Web site. First off, the Visa site asks users to enter their credit card number. Then there's the fact that when I clicked on any of the links on the Verified by Visa site, I received "Page not found" errors.

**Update, 2:13 p.m. ET:** Looks like the site has been shut down, no doubt thanks to the hard work of the folks at the [SANS Internet Storm Center](#), who first spotted this scam.

Also, I heard back from Geotrust. **Joan Lockhart**, the company's vice president of marketing, said the site was registered on Sunday and the cert was issued early this morning. Lockhart said Geotrust has a rigorous process in place to check for phishy certificate requests that relies on algorithms which check cert requests for certain words, misspellings or phrases that may indicate a phisher is involved. In this case, she said, the technology did not flag the request because there was nothing in the Internet address to indicate the site was at all related to a financial institution.

Geotrust's cert verification process is largely automated: when someone requests a cert for a particular site, the company sends an e-mail to the address included in the Web site's registrar records, along with a special code that the recipient needs to phone in to complete the process.

Lockhart said she doubted that inserting a human into that process would have flagged the account as suspicious.

"I would argue that probably anyone who is processing mountain-america.net would not have raised flags," she said.

**By Brian Krebs | February 13, 2006; 01:50 PM ET | Category: [Fraud](#)**

---