



VbyV password reset is childishly simple

Hit keyboard with fists, gain access

By John Leyden

Posted in [ID](#), 23rd October 2008 10:56 GMT

Much was made of how easy it was for a hacker to reset Sarah Palin's webmail account password and gain illicit access to emails, but resetting passwords for Verified by Visa - which supposedly makes online transactions more secure - is arguably even easier.

To reset Palin's email account a hacker needed to know the Republican VP candidate's birth date, her zip code and the answer to a secret question on where she met her husband. Resetting a Verified by Visa password, by contrast, requires only card details and a date of birth, an issue highlighted to an earlier *Reg* [story](#) on the scheme.

Reg commenter Anthony explains.

Barclays Verified by Visa allows anyone who has the credit card in their hands to set a new password for VbV with just the card details and the card owner's date of birth. Since the latter is trivial to discover for most people, this adds almost no additional security to the process.

Reg reader Jusme reports the same issue.

Verified by Visa is one of the reasons I no longer use Barclaycard. Pretty much every time I had to use it the password was not recognised and I had to "reset it", which just meant entering my DOB and a new password, hardly very secure.

The issue has been noted, and [commented](#) on in the blogosphere as far back as June, but has received little attention in the mainstream media, despite the obvious security implications.

Punters can simply re-enroll onto the scheme, gaining multiple passwords in the process, David Harper reports. UK banking association APACS disputes this point, while conceding there's a case to be made for improving the password reset function that goes alongside 3DSecure.

Because of the password strength for the verified by visa scheme forcing you to use two digits I of course had forgotten it.

Imagine my surprise then when I found out I could click on the enrollment link and re-signup. Now I got to the point where I could enter a password and got the error back saying "Must include 2 digits". This acted as a reminder to what my password was so I tried that - after which I got "You've already used that password" - so I gave up re-enrollment at that point.

However it seems that it's completely unsecure if at any point you can enroll in the scheme and create a new password!

One anonymous commenter reports that he's managed to create more than 10 passwords.

The thing i don't understand is how easy it is to make a new password, anyone with your DOB and card could easily just do it themselves anyway, I have made a new password about 10 times as I can never remember it.

To be honest, given that its so easy to do it, this 'steve' isn't proving anything to anyone by not just enrolling, he's just caused himself a load of hassle by making himself look dodgy (as is the point of the system, im actually somewhat encouraged that this thing seemingly would do something if someone had actually acquired /some/ of my details) and not bought a load of things he would've liked to, well done!

Andrew Goodwill, a director at card fraud prevention specialists The 3rd Man confirmed that resetting a user's Verified by Visa password requires knowledge of only a user's birthday and the corresponding card details.

"Both Verified by Visa and MasterCard SecureCode are based on 3D Secure protocol checks. There needs to be a consistent way to reset passwords and date of birth has been chosen as the only data needed to carry out a reset," Goodwill explained.

A spokeswoman for banking association APACS questioned this reading, and said that how password reset functions work has more to do with the way in which individual banks apply their systems than the 3D Secure protocol itself. She said our questions were better put to either Visa or MasterCard, while offering some general observations on the 3D Secure scheme.

"What individual card companies do in introducing the technology is competitive but, speaking generally, they have a need to balance a requirement to make resetting password straightforward with security. Generally they use a mix of on-card and off-card data," she explained.

"We're at the early stages of this system so we need something that allows people to re-register easily. As people get more used to it customer authentication can be ramped up. Some banks are already introducing two-factor authentication for online transactions."

More than 25 million UK-issued credit and debit cards are registered with either Verified by Visa or MasterCard SecureCode, according to APACS stats [published](#) late last month. Merchants signed up to the program collectively account for a third of UK ecommerce sales.

Over the last two years the number of UK-issued cards registered through the scheme has increased by a factor of seven. Ordinary customers have a legitimate interest in the security of passwords issued through Verified by Visa and MasterCard SecureCode - particularly when purchases made using the scheme bear an additional mark of authenticity that may make it harder for legitimate customers to establish they were not responsible for fraudulent transactions made using purloined credit card credentials.

Visa and MasterCard ought to be able to defend the password resetting regime they have established, but neither organisation responded to our request for comment at the time of going to press. ®