Why You Should Enable Two-Factor Authentication For Google Apps and GMail

Posted At : August 12, 2012 1:41 PM | Posted By : Stefan Richter
Related Categories: Google

If you are running your emails through a Google Apps account and are not using two-factor authentication then **now may be a good time to do so**.

Keeping on top of one's online security can be challenging, but protecting your email account from unauthorised access is crucial since most sites and systems fall back onto email for account password recovery. This means that once a hacker has access to your email account they can use it to gain access to your Twitter account, Facebook, potentially other email accounts and in some cases even cause you to lose your data as the recent case of **Matt Honan** dramatically demonstrates.

So why exactly is two-factor authentication so much more secure than a normal (even a super-strong) password? The answer is pretty simple: in addition to having to supply a piece of information ('something you know' such as your password), using two-factor-authentication requires you to supplement the password with 'something you have' such as a one-time-use token which proves that you are in possession of your phone (in the case of using Google Authenticator or SMS tokens) or your keyfob (in the case of online banking and Paypal for example).

With two-factor-authentication turned on, a hacker would require to not only know your password but would also have to be in possession of your phone or keyfob. This raises the bar significantly and would have protected Matt's GMail account even if the hackers would have managed to reset his password.

I've been using **two-factor authentication** for quite some time for various accounts such as my Google Account (I've got one for GMail and also a Google Apps account), Paypal (where I had to buy the one-time-use token generating keyfob), Amazon Web Services (again, I had to pay for the keyfob but it's a price worth paying and I believe you can now also use the free **Google Authenticator** app) and of course various bank accounts where my bank supplied the token-generating device for free.

So how do you set up two-factor authentication? For GMail it's **pretty simple** and Google have even posted a **video describing the process**. As you may have seen in the video, some applications - including most mobile email accounts - will require you to set up special application-specific passwords as these applications lack the ability for the user to enter a one-time use token. Granted, this can be a hassle but I recommend you give it a try, once set up these accounts require little maintenance in terms of password management and a compromised application-specific password won't give anyone access to your actual account.

For Google Apps the setup process is slightly more challenging as firstly your Google Apps Account Admin needs to enable the option for two-factor authentication on the account level.
To do that log on as Google Apps Account Admin at www.google.com/a/YOURDOMAIN (substituting YOURDOMAIN with your actual domain - doh!) and choose 'Advanced tools'. Scroll down a little bit, find the Authentication section and check the 'Allow

users to turn on 2-step authentication' option.

Once done you (or your domain admin) need to tell the Apps account users to turn on two-factor authentication under their Google Apps user account. That **process is described here** and is similar to the setup for two-factor authentication under GMail.

Hopefully these instructions are useful and have encouraged you to secure your email account.

Please leave a comment if you run into any issues, or have some additional tips to share. If you found this post useful then i'd much appreciate a **tweet about it**. Thanks!