Gamigo Password Leak: When Security Fails Swift Action is Critical

By Denise Richardson

Another data breach is in the news, this one from the online gaming site Gamigo. Approximately 8 million email accounts and user passwords have been leaked recently, dwarfing the size of breaches like the recent Yahoo! Voices breach. This story is a little different than most if not all of the similar breaches of the last year or two, though, and Gamigo actually let their users know about the breach months ago even though the data is just now finding its way online.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Unlike the Yahoo! Voices breach and breaches of companies like Sony last year, the Gamigo passwords that were stolen were encrypted so they would be harder for someone who finds them online to use. Resourceful hackers can overcome the encryption, however; according to Forbes, a hacker had cracked around 94% of the passwords within half an hour of the list making its way online. Fortunately, in this case having the passwords might not do hackers a lot of good as far as getting access to Gamigo accounts goes.

When the breach was first detected four months ago, Gamigo made its users update their passwords as a preemptive measure. When the stolen email addresses and passwords didn't show up online right away some might have wondered whether it was excessive for them to force password changes at the time, but now that the passwords have been leaked there are probably a lot of Gamigo users who are glad that the company took the steps it did.

Of course, the problem of users using the same email and password combinations for other sites still exists. As I mentioned in my recent post about the Yahoo! Voices breach, hackers don't just use stolen email addresses and passwords to try and gain access to a single account; they'll try the same combination on other sites as well. While a Gamigo user might not be worried about his game account, he won't consider that at this very moment a hacker might be trying out his information on eBay, or PayPal, or Amazon or even Netflix. If the same login information is used on multiple sites then it puts you at risk if any of those sites are compromised.

If you've been using the same passwords and login credentials on multiple sites, then please reconsider this practice. You don't want the mistakes of one website to put you at risk everywhere on the Internet. Here are a few things that you can do to try and keep yourself safe when it comes to your login information:

Create unique passwords for every website that you visit. If you want to make the passwords easy to remember, associate a seemingly-random word with each site and incorporate that word into your password; just make sure that it's not obvious and that it's not the entire password.

Add capital letters, numbers and an array symbols to your passwords. Even a password like "Apple-567" will be harder for someone to guess than just "apple."

Use free email services to make new email accounts that are specific to the sites that you sign up for. This practice could be seen in action with the Gamigo breach, as 5000 of the stolen email addresses contained the word "Gamigo" in their names.

Use online password randomization and storage sites or software that's designed for the same purpose. This allows you to have a master account with a single password but have completely randomized passwords for the actual sites that you visit. You can expect to hear more about this soon, as I plan to review some of the websites and software solutions that are available to help you stay safe online.

Change your passwords regularly, and always change your passwords when you hear about a data breach at a site you've frequented. Even if you're not an active member, you never know whether your information is still in a database somewhere.

Getting back to Gamigo for just a second, I just wanted to wrap this up by saying how refreshing it is when I see a company taking responsibility for their actions after a breach like this and not just waiting to see what the fallout is before taking action. The Gamigo breach puts me in mind of the University of Nebraska breach that I told you about back in June; while it likely could have been prevented, the company was transparent about what had happened and took action to prevent further damage even before news of the breach broke. I hope that more companies follow their example in the future when their security fails.

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow ACCESS