Personal and Private Data Continues to Leak from Sony

Posted on Dec 22, Posted by Ira Greene Category Security

This holiday season might leave technology and entertainment supergiant Sony with nothing but a big lump of coal in its stocking. In a high-profile hack, hackers continue to leak Sony's employees' sensitive information like Social Security numbers, passports, and even personal emails. This is obviously an issue for the company, but so is its lack of IT security, as shown by their passwords being stored in a folder named "Passwords."

When the server was hacked and its contents were made visible to the attackers, it's understandable that they would make a break for the folder titled, "Passwords." They probably thought Christmas came early with this convenient present, gift-wrapped and ready to be consumed by the ravenous masses. At the rate at which data is being leaked, it's hard to guess what information will be exposed next.

GOP (Guardians of Peace), the group supposedly responsible for the hack, has announced that if Sony employees or associates don't want their personal information leaked, they should email them directly requesting to not do so. Considering the extremely personal nature of this information, it wouldn't be surprising to see some people throw in the towel.

Some folks, like actors Seth Rogen and James Franco, are taking advantage of the hacks by making jokes on *Saturday Night Live* and social media. This distracts others from the gravity of the situation. This hack is a big deal, and crazy amounts of confidential data could leak due to lackluster security practices. All of this could have been avoided by optimizing both network security and password-keeping best practices. Here are some of the best ways to keep your

passwords and sensitive information safe from prying eyes:

- **Use complex strings of characters, numbers, and symbols**. Stay away from simple words like “admin” and “password” when creating your login credentials. In fact, a lot of institutions will force you to use passwords of a certain length, with numbers and special symbols. The reason? It makes it more difficult for hackers to guess it and obtain it. One simple way of strengthening your password is by plugging in numbers where certain letters would normally be, like 1 instead of a capital I.

- **Use long passwords rather than short ones**. This goes back to many websites requiring a certain number of characters (many use a minimum of eight). It makes sense that a longer password would be more secure than a shorter one. For instance, a short and easy-to-remember password can easily be guessed by a hacker, and when they are trying millions of different character combinations all at once, it’s no surprise that a weak password can be compromised fairly easily.
- **Invent words when possible**. Using common words can make your password vulnerable to a dictionary attack, where a hacker attempts to crack the lock by rapidly plugging in common words. To protect your business from this possibility, use made-up words. This complicates the hacker’s process, forcing them to either give up or try something else entirely.

- **Don’t use easily-obtainable information**. Some people like to use their date of birth or Social Security number as their password. This is generally a bad practice. Both of these, with enough digging on the hacker’s part, can be figured out; plus, on the flipside of things, if a hacker uses keylogging to discover the characters behind your password, you can kiss your identity (and login credentials) goodbye.
- **Never use the same password twice**. With such a complex password, it might be logical to assume that you should use the same password for everything, seeing how difficult it is to remember. This is a bad move. If a hacker compromises one account, they’ll try to use the same password for your other logins. If everything is the same, it’s game over. You want to use multiple different passwords for all of your accounts.

Let a Password Management Solution Remember Your Passwords For You

All of these best practices can make your password difficult to remember and even more difficult to guess on the fly. Granted, it’s tough to remember even one complex password. Thankfully, Lighthouse Technology Solutions’s preferred password management solution makes remembering even complex passwords easy as can be. A password manager is an application where all of your passwords are securely stored. When they are needed, the application plugs the necessary credentials into the website you’re visiting, giving you safe and easy access to your account.

If this sounds like too much of a hassle, another less-secure option is to write down all of your passwords in one place, like a notebook or a post-it note. However, as seen from Sony's blunder, you absolutely can't label the list as passwords. For more information about how to keep your data safe in a world full of criminals, give us a call at 703-533-LTSI (5874).

Tags: Tagged in: Hackers Passwords Security