Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=lessons-of-ashley-madison-how-crackable-are-your-passwords

Lessons of Ashley Madison: How "Crackable" Are Your Passwords?

Posted October 20, 2015

The well-publicized recent hack of the Ashley Madison website will probably earn a spot in a "Hacking Hall of Shame"—alongside the infamous Sony and Target breaches—for the sheer amount of grief it may cause millions of marriages. Most of the blame lies with the Ashley Madison administrators for leaving their users' data vulnerable to a full-scale cybertheft. But it also brings to light how many careless users jeopardized their marriages by relying on **unsecure, easy-to-guess passwords**.

A Word of Warning

Security expert Dean Pierce wondered how many encrypted Ashley Madison passwords he could decipher using a "cracking rig"—a milk crate-sized hardware contraption typically available on the black market for around $1,500. After adding some fairly elementary programming instructions, Pierce's cracking rig began sifting through the massive volumes of code publicly exposed from Ashley Madison's servers. In just over five days, he'd already retrieved 4,000 user passwords—about 32 per hour—at which point he decided to stop the experiment.

What were the most common passwords revealed from Ashley Madison's clientele?

"123456": 202 users

"password": 105 users

“qwerty”: 32 users

“12345678”: 31 users

“ashley”: 28 users

If these users carelessly risked their spouse’s trust on the most easily “guessable” passwords, how often did they use similar passwords for social media, retail websites, online bank accounts, or protected data at work? It cannot be stressed enough: **Strong passwords are the backbone of personal computer security.**

The key to choosing a “crack-resistant” password is to understand how passwords are usually hacked. A typical password consists of a single English language word—a proper name, a noun, or anything else in the dictionary—combined with an “appendage,” most often a suffix, such as:

- “!” or other punctuation marks
- One or more digits
- Common web abbreviations (“4U,” “LOL”)

Malicious hackers around the world equip themselves with sophisticated tools which can test millions of word/suffix combinations *per second*—much more powerful than the $1,500 cracking rig—until they stumble upon users’ weakest passwords.

Have you used the names of your kids as passwords? You’d be surprised at how many of your personal connections—family members, neighbors, and more—are now easily divulged on various “people search” websites. A determined hacker will assume those names are prime password material. Same for your birthday, phone number, or street number/zip code.

How to Pass the Test

If hackers are on the prowl for predictable words, one strategy for creating a guess-proof password is to use an **acronym for a sentence or phrase**. For example:

“TCJOTM” for “the cow jumped over the moon”

“ANWYCCDFY” for “ask not what your country can do for you”

…or a description of something else you’ll remember easily.

The more characters in a password—upper and lower case, plus special symbols—the greater the level of security. One useful tool for testing a password is Microsoft's free password checker. Never settle on a password rated less than "Strong."

For help with any security-related IT issues, get in touch with us today.