Secure Passwords: The Rules Have Changed

By Sharon D. Nelson, Esq. and John W. Simek

Passwords might seem a tired subject to some, but the rules of the security game have changed – and it is high time to say goodbye to those wimpy, eight-character passwords. If you are using less than eight letters, shame on you!

So why the major change?

According to a report recently published by the Georgia Institute of Technology, it is time to move to 12 character passwords. In essence, Institute researchers were able to use clusters of graphic cards to crack eight-character passwords in less than two hours. And trust us, if researchers are doing this, so are the cybercriminals of the world.

The researchers discovered that, when they applied the same processing power to 12-character passwords, it would take 17,134 years to crack them. Cybercriminals, even when highly motivated, are going to bypass 12-character passwords – there are just too many folks with out there asking for their security to be violated with less secure passwords.

Richard Boyd, a senior research scientist who worked on the project, says that 12-character passwords should be the de facto standard we all use. It is simply too clear that the degree of your vulnerability is dictated in large part by the length of your password. Sad, but true.

The recommendation really strikes a balance between convenience and security – and assumes that password-cracking capabilities will continue to increase, as has certainly been true since computers became an integral part of our lives.

Here's how they came to their recommendation: They assumed a sophisticated hacker might be able to try 1 trillion password combinations per second. If that were the case, it would take180 years to crack an 11-character password. If you add just one more character, it would now take17,134 years to break the password. Given that the computing power of those with evil intent continues to accelerate, that added character gives (for the foreseeable future) a pretty good level of security. We are always asked, "When will the rules change again?" We sure wish we could tell you, but that's a mystery even to the experts. It's not just an increase in processing power that makes it hard to predict – it is also harnessing the power of the cloud – something that the hackers are beginning to exploit. When the rules do change you can be sure we'll write another article!

For many years, we have lectured about passwords to audiences of lawyers. In the beginning, it was very frustrating, as lawyers wanted "instant on" information and were unwilling to take passwords very seriously. This is still true in the case of smartphones. Consistently, when we poll lawyer audiences, more than half do not have a PIN (personal

identification number) on their smartphone. They simply want that “instant on” access. That’s fine until you lose your phone, which is a tremendously common experience. Now the person that finds your smartphone also has “instant on” access to all your data. Not a terribly effective way to safeguard your confidential data.

Make no mistake about it, without a PIN, someone with evil intent will have access not only to data that you yourself could see on your phone, but to whatever deleted data may reside within its memory. This is precisely what we do in computer forensics lab when phones come in as part of the discovery process, albeit without the evil intent!

Apart from smartphones, lawyers have generally gotten smarter about passwords over time and tend not to use the names of children, sports teams, etc. as their passwords. We still find passwords on sticky notes on monitors or in desk drawers. That is an unending source of despair to all security experts, but apparently most of us cannot remember our passwords – and indeed, we have a lot of sympathy for the fact that lawyers have so many passwords that it hard to remember them all.

In response, over the last few years, we have joined others who lecture on security and recommended the use of full sentences or passphrases as passwords. They are so much easier for all of us to recall.

“I’msickofLindsayLohan!” is simple enough to remember and complex enough to confound a would-be password cracker. Using characters that are non-letters helps add to the complexity and therefore to your security. The English alphabet contains just 26 letters but there are 95 letters and symbols on a standard keyboard. “Mixing it up” makes it even more difficulty for computers to break your password.

Some, including Microsoft, will argue that users should not use real words or logical combinations of letters because they may be guessed by a “dictionary attack” using a database of words and common character sequences. Maybe, but we think that is overkill unless you’re dealing with national security data or the formula for Coca-Cola.

The research used at Georgia Tech was a “brute force” attack, meaning that they simply tried all possible combinations of characters. The computer graphics cards they deployed are very cheap and easily programmed to perform these sorts of computations. The processors in the cards all run simultaneously, working to crack the passwords. Amazingly, these processors, running together, now have the processing power of what we used to call “supercomputers.”

So let’s say you accept the need for 12-character passwords. Several issues arise. One is that your bank, your stock brokerage, etc. may not allow for 12 character passwords. There are a lot of websites out there that still do not permit long passwords, though with each passing day, that is changing.

More problematic is that many sites do not **enforce** the long passwords. They may accept a six letter password or they may not insist that you use non-letter characters. This

remains a significant problem, as many sites containing sensitive data have not yet caught up with security requirements for the coming decade.

Perhaps the greatest problem is remembering all these passwords. One solution is to use an encrypted flash drive such as the IronKey, which includes a password "vault" application that remembers all the characters for you. This has been our solution, which is great – until we forget the IronKey. We can only sigh remembering how many times **that** has happened - fortunately we've always been in the same city as the IronKey. We haven't managed to lose our IronKeys yet, but as small as they are, that would also be easy. There is an insurance policy – you can store your passwords (encrypted) on the IronKey site. But you can sense that there is a nuisance factor here.

There are websites which will store your passwords for you, but then you must trust the security levels (and employees) of that website.

Particularly dangerous are social media passwords, which are often used to log in all over the Web. Adding to the danger is that fact that third party applications regularly require you to turn over your social media ID and password so that they can have interaction between say, Facebook, and the popular applications Mafia Wars and Farmville are good examples. This makes things easy for the user, but now a cybercriminal with a single set of credentials may be able to access multiple sources of information.

For $19.95, you can turn to a product like eWallet (http://www.iliumsoft.com/site/ew/ewallet.php) which will store your passwords in encrypted format and allow you to sync access to it from multiple devices, including smartphones (be sure to check that yours is supported). This may be the best solution currently available for busy lawyers. John uses eWallet as a backup (synced to the BlackBerry) to his IronKey. With a 30-day free trial, it's hard to go wrong. There are similar products out there, but research them carefully before selecting one. Most have been tested by independent sources – your best way of screening software since all vendors will trumpet their products as "the" solution to your problems.

Is there a way to store passwords on your own system securely? Well, it will help considerably if you store your passwords in a Word document or Excel spreadsheet that is itself password protected. This means that the data will be stored in encrypted format IF you have Office 2007 or later. You still need to make sure that the password you use to protect the file is very strong and not the name of your pet cat.

So what if you are asked, while browsing the Web, if you'd like to store your ID and password on the computer being used? Don't do it. If – however it happens – your machine is compromised or someone who has the keys to your network gets on your computer, you've given someone else the power to "be you" on any site where you've asked to have the ID and password stored.

Do you need 12 character passwords to access websites? For anything important, of course. You sure wouldn't want to access your bank, your stock market account or your retirement account without a strong password. Ditto for anywhere you shop since many

of us save credit account information on the site so that we can make purchases quickly. And for heaven's sake, don't use the same ID and password on different sites – once one is compromised, so are the rest if you take that perilous route.

Whatever you do, make sure you do take passwords seriously. We know from experience that most lawyers are not going to buy a product like the IronKey or use a product like eWallet. This may change as the years go by, but for now, the majority will simply come up with passwords on the fly as required. If that sounds like you, at least take heed of the message conveyed by the Georgia Institute of Technology and make your passwords strong 12-character passwords. At least then you will have demonstrated that you took "reasonable measures" to protect client confidentiality.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com

.