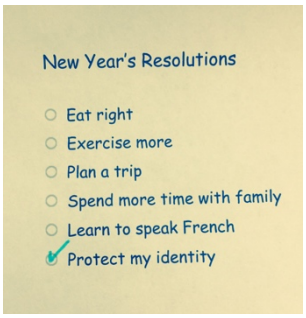
This Year, Resolve to Protect Your Identity

Deke Kassabian, Information Services & Technology Division



The start of a year is a great time to take stock and to commit (or re-commit) to the things that matter to us. That's probably why so many of us write New Year's Resolutions. Whether we write them down, share them with friends, post them on social media, or just silently commit to them without sharing, New Year's Resolutions can be a way to identify what's important to us and how we can improve and be the person we want to be.

I almost always resolve to diet and exercise hoping to lose weight. It often works, too, at least for a few months. I usually write a few other self-improvement resolutions such as reading some of the books that have been on my list for a while, or to devote more time to playing the piano. I have friends who have resolved to learn or brush-up on a foreign language, spend more time with family members, or to take on a specific physical challenge such as to run a marathon or hike part of the Appalachian Trail.

May I suggest a resolution? This year, resolve to better protect your identity. There are some very practical steps you can take. I'll list a few here and invite you to suggest and share some others. Many, but not all, have to do with passwords. Any of these in isolation can help, and doing some combination of them can help even more.

1. **Choose good passwords and passphrases.** Longer passwords and more complex passwords can both help to protect against "brute force attacks" in which a hacker tries to guess your password. Certainly, avoid very short and simple passwords. If a service allows very long passwords and doesn't require complexity (uppercase, lowercase, numeric, special characters), you might use a ***pass phrase*** which is a long string of words that are meaningful and memorable to you, but that would be hard to guess. If complexity is required, you might try a password generator (built into some browsers and applications) to suggest a password, or perhaps base your new password on a long phrase by taking the first letter of each word and making a single acronym and then swapping some of the letters with numbers or special characters. Finally, add some additional characters to the beginning and end.
2. **Avoid using the same password for multiple services.** Whatever password you choose in step 1, it is best not to use that same password for more than one service. If an online service somehow allows your password to be compromised, it would be better if the compromise were limited to just that one service rather than several services for which you have used that same password.
3. **Use a password vault application.** When you take the first two items above into consideration, you very likely will have the need to safely manage many different long or complicated passwords. Don't write them down. Pick a good ***password vault*** application that can store and protect your passwords in an encrypted storage. The best password vault applications can even generate/suggest passwords, sync passwords across your computers, smartphones and tablets, and even auto-fill fields in web applications if you choose to enable that feature.
4. **Be careful about "password recovery questions."** Password recovery questions such as "what is your mother's maiden name?" and "what was your first pet's name?" are often used to allow you to prove your identity to recover a forgotten password. This can be very handy. Unfortunately, it can also lead to account compromises when someone else guesses the answers. In the most extreme example of problems with password recovery questions, a major hack of Yahoo information led to not only passwords but password recovery questions and answers to be

compromised. The result? The questions and answers you use on Yahoo and *perhaps many other services* wind up in the hands of the bad guys. In the worst case, they could use what they learned in the Yahoo hack to log into your unrelated accounts!

5. **Try two-factor-authentication where available.** Some services will allow you to use more than one "factor" to prove your identity. One factor may be a password, while another may be a string of numbers or letters sent to a smartphone or other device in your possession that you are then asked to enter on the login screen. In this way, login is only possible by someone who both ***has the device*** and ***knows the password***. Something you have, and something you know, are the two factors. This greatly improves security at the cost of a small extra step during login.
6. **Be suspicious of email that invites you to log into a service.** Hackers send email messages that invite users to either send their login information or invite them to connect to a page that looks very much like a legitimate service login page but that can be used to capture usernames and associated password. This attack on user identity is called phishing and it has become a major risk on the Internet. We recommend that you not click links in email messages in such cases. If your bank or employer seems to have sent an email message asking you to connect and log in, use your browser to connect to that service via a known address, and make sure the URL that shows up in your browser is the location you expect before logging in.
7. **Avoid giving out your social security number.** Social security numbers have been used for many years as a unique identifier by many services, online and off line. Unfortunately, this practice has allowed criminals to combine this information with other less sensitive information like birthday and address to achieve identity theft at banks. When you are asked to supply a social security number other than to an employer or a financial institution, it is reasonable to push back, express concern, and ask about alternatives. This practice may help you to avoid identity theft.

These are just a few of the important ways available to help protect your online (and offline) identity. Perhaps you have been using passwords to access email and web services for many years and have established practices and patterns since before identity risks rose to today's levels. Now, armed with better information and better tools, it is possible to do more to protect your identity, and I believe that revisiting your practices is truly in your best interests. These can be resolutions that really work for the long term. If only I could say the same for my diet and exercise resolutions!

Do you have other suggestions to help protect identity information? Send us your thoughts.