COMPUTER BYTES – INTERNET SECURITY

By: Harv Oliver

Happy New Year to all! Here's hoping your personal and business endeavors for 2016 are rewarding and successful.

Last time we talked about security. This time I'm expanding on one of the items, "Internet Security". With 2016 under way, password management company *SplashData has released its annual round-up of the worst passwords of 2015.

The report is based on more than 2 million passwords that leaked online during the year. It's true some sites are forcing us to put in stronger passwords, still, one trend found in 2015 is that while users are coming up with longer passwords they are simple and not random. Two examples the company references are '1234567890' and 'qwertyuiop' (this is trick of using the top row of alpha keys on a standard keyboard).

The more common practice of not creating strong passwords remains including basic numerical passwords and sports terms. The new *Star Wars* was big in 2015 and it seems quite a few people went with *Star Wars*-themed passwords such as 'starwars,' 'solo,' and 'princess.'

Here's Splashdata's complete list of the 25 worst passwords for 2015, with their ranking from 2014 in brackets:

1. 123456 (Unchanged)
2. password (Unchanged)
3. 12345678 (Up 1)
4. qwerty (Up 1)
5. 12345 (Down 2)
6. 123456789 (Unchanged)
7. football (Up 3)
8. 1234 (Down 1)
9. 1234567 (Up 2)
10. baseball (Down 2)
11. welcome (New)
12. 1234567890 (New)
13. abc123 (Up 1)
14. 111111 (Up 1)
15. 1qaz2wsx (New)
16. dragon (Down 7)
17. master (Up 2)
18. monkey (Down 6)
19. letmein (Down 6)
20. login (New)
21. princess (New)
22. qwertyuiop (New)
23. solo (New)
24. passw0rd (New)
25. starwars (New)

You KNOW some of you are finding your password(s) in the list!

There's no doubt about it, managing passwords is a pain, but they're the best security measure available right now. Tech companies are working to change that, but at the moment there's no getting around the need for good, strong passwords. I'm sure many of you have heard this before but it still needs repeating and most of all addressed.

The best thing to do is create long, *random* passwords that are hard to guess. Your passwords should use a combination of letters (including different cases), numbers, and symbols if possible. Also make sure you use a unique password for *every* major account you have including banking, email, Paypal, social networks, and any website that has your credit card data, such as Amazon.

If you have trouble remembering those new passwords you might try a password manager such as KeePass, LastPass, Dashlane, or SplashID.   Generally speaking, these tools allow you to install their application, create a strong master password, then start saving and auto filling passwords for every website. You then have different passwords for different sites but they're managed with one killer strong password. Again, you don't want to tell people "I use the same password for everything." Should they get it, they now have access to ALL your stuff!

You should also use **multi-factor authentication whenever it's offered to keep your accounts extra safe. That way if you ever lose control of your password hackers will find it extremely difficult to get into your account(s). Most major services support multi-factor authentication, including Amazon, Facebook, Gmail, Microsoft, and Twitter.

If you stick to the basics keeping your accounts secure is not that hard—and sticking to best practices will save you from headaches should your account credentials end up in the hands of hackers.

NOTE: Our sharing of information within articles includes suggestions and tips. USE AND/OR APPLY AT YOUR OWN RISK. If you have any questions or concerns, please contact our offices for professional service/guidance. Until next time, don't forget your backups! For more information, contact Harv Oliver, HANDS-ON Consultations, (805) 524-5278, www.hocsupport.com

*SplashData has been a leading provider of security applications and services for over 10 years. The company's secure password and record management solution SplashID Safe has over 1 million individual users worldwide as well as hundreds of business and enterprise clients. SplashData was founded in 2000 and is based in Los Gatos, CA.

** Multi-factor authentication (MFA) is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism - typically at least two of the following categories: knowledge (something they know); possession (something they have), and inherence (something they are).