

Security Tips for May

By David Shulman, WPCUG Weekly Update editor, intergroup liaison, and a co-organizer of the WPCUG Meetup page.

May 2018 issue, WestchesterPCNews

www.wpcug.org

[wpcug.d_shulman \(at\) yahoo.com](mailto:wpcug.d_shulman@yahoo.com)

Are the headlines, describing one security breach upon another, causing you to pay attention? As a result, this column has been added to the newsletter.

I CONTINUE to be flabbergasted and upset by the news each month.

Where to begin? Saks Fifth Avenue? Lord and Taylor? Delta? Sears? Panera? Facebook?

I'm "thrilled" by the wonderful competence of all those "private sector" companies who are busy telling all their friends in the entertainment world (you know the channel) how competent they are and how poorly behaved the public sector is.

ONE—Passwords. Use individual ones everywhere. Too much trouble, you say? Your biographical data is collected by each account you create, and the aggregate of this data is VERY powerful. USE A PASSWORD MANAGEMENT PROGRAM. It creates unique, complicated passwords for each place that needs one. The entire thing is kept under ONE password that you need to remember. All the rest is facilitated by the software.

TWO—Lie everywhere. Yes, you read that right. DO NOT give away your mother's maiden name, your birthday, license number, first public school, childhood address, best friend, your Social Security number, etc.

Give away NOTHING. Why should you? Either make up the same answers everywhere or annotate unique ones in your password manager. If you make it up and use it everywhere, you are back in the same trap.

THREE—Blind your webcam. You do not want someone to look around your house, at you, and invade your computer as well because once they can see your keyboard...

FOUR—Think seriously about those devices that you can talk to. THEY LISTEN ALL THE TIME. You know how much more convenient it was when TV channel changing was done with remote control (instead of using one of your kids)? Don't assume that Alexa or Siri or Echo are as benign as the remote control! At the very least, tremendous data is being gathered. You forget that you are being listened to. You say things that you might NEVER say if there was a houseguest. Passwords, birthdates, account numbers, etc., are ALL on the table (or in someone's ear).

FIVE—Don't stay signed in to your accounts or your computer. No good can come from that and you save merely seconds. A stolen laptop or computer is an open door TO YOUR IDENTITY. So is a computer that is logged in because you had to use the bathroom when you are not alone—even at home.

SIX—Check your logon records. On Facebook, see the activity logs; on Twitter you can access analytics.twitter.com

SEVEN—App permissions. Check on your Android or iPhone to see which apps have permissions. Do they need the permissions? All the time?

LASTLY—UPDATE YOUR STUFF. Why do you think the folks who work there get paid to do this? It's because the company's rear end is on the line, that's why! So is yours if you can't find the time.

OBTW—DON'T FORGET TO PERFORM BACKUPS. Automating them is better.