

Security Tips for June

By David Shulman, WPCUG Weekly Update Editor, Westchester PCUG

June 2018 issue, WestchesterPCNews

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

The June issue of Consumer Reports has a cover story entitled “Protect Yourself from Scams” and a subhead containing the words “smishing, spoofing, and shimmers.” Intriguing? Get a copy. As a bonus there is an article on the protection of your financial data after the Equifax incident. Did you know that 52 percent of surveyed Americans have done nothing in response to that incredible mess?

Traveling and staying in a hotel with an electronic door lock? A team from F-Secure has created a hack (after one of them had his laptop stolen from his room years ago) that takes about a minute and creates a master key for all the rooms in a hotel. This hack still is effective in some hotels. Read up!! <https://www.wired.com/story/one-minute-attack-lethackers-spoof-hotel-master-keys/>

Oath is the new entity in charge of what formerly was Yahoo, AOL, and Verizon email services. Oath has a new privacy policy. That’s what you have NEVER read, skipped to the end of, and signed. Kim Komando has gone crazy over the details and perhaps so should you! Oath apparently claims rights to pictures and to analyze financial data in your mail. See <https://www.komando.com/happeningnow/455054/yahoo-aol-and-oaths-new-massiveemail-privacy-policy-changes-you-need-to-knowabout>

Delta Airlines and Sears were hacked last fall. If you shopped there or booked a flight, the software company [24]7 revealed complete profiles of well over 100,000 customers. It took months for them to reveal this theft. The worst example of delay this month has come from Panera Bread. Apparently, they were notified last August of a breach, but it took until mid-April 2018 for them to act. The data stolen affected over 30 million customers and contained names, addresses (email and physical), birthdays, and the last four digits of credit cards leaked onto the internet.

What to do?

- Stay on top of your credit card purchases. Set alerts to your cellphone. Check the statements regularly.
- Be alert about mailed offers of credit and calls from credit card or banking folk. They may be scams using your stolen data to gain your trust. Consider a credit freeze on all the credit services. You can lift it when you need to.
- Make sure your mail (your USPS “snail” mail) is secure. If your mailbox can be accessed by anyone walking down the street, consider steps to lock it up or use a secure mailing address such as a post office box. Thieves use your ID to apply for credit cards and then steal them from your mailbox, activate them, and have a shopping spree. While it is true that you are not responsible, the hassle of proving it was not you and cleaning this up is incredible.

Consider this: Increasingly, vendors are forcing you to stipulate that any disputes between you and them be resolved by an arbitrator of their choice as your only recourse. Historically, this method has not worked in the favor of the customer. Legislation has been introduced to nullify this condition. When your security is compromised, and you not only have to fight the people using it but the company that compromised it, that's an unfair burden.