



The Monthly Brief

Volume 6 Issue 1

January 2018

CYBER SECURITY RESOLUTION

Data breaches and scams show no signs of slowing in 2018. Maybe it's time to add a "Cyber Fitness" resolution and up your game to protect your personal identity.

According to a Javelin Strategy 2017 fraud study, more than \$107 BILLION has been stolen from consumers by identity thieves in the past six years.

[PNC Bank](#) recently published the Top Six New Year Resolutions to help protect your identity.

Keep Software Updated by installing the latest security enhancements and patches. Always use security, malware, and anti-virus protection when going online.

Use Secure Sites only for online shopping. These sites display https://: at the front of the web address. The "s" stands for secure.

Update Passwords more frequently and anytime there has been a security breach. Make sure their strong and varied from site to site.

Security Alerts Sign up for alerts via text message or email to inform you when important activity on your credit card or banking account occurs.

Use Two Step Authentication A unique one-time passcode that is automatically sent to you via text message every time you logon online to your bank account.

Review Your Credit Report Get a free copy of your credit report every 12 months from each of the 3 national credit reporting agencies at annualcreditreport.com.

Follow Us On Facebook

Subscribe: philarcher@sa18.org

New Data Breach

Just days ago, Ancestry.com confirmed that a server on its RootsWeb service exposed a file that had usernames, email addresses and passwords of 300,000 registered users.



In an [official statement](#) released by Ancestry.com's Chief Information Security Officer Tony Blackham, they have confirmed that the file does contain the login credentials of the users of RootWeb's surname list information. To protect its users, Ancestry has locked out the accounts of the customers who used the same credentials on RootsWeb's surname list and Ancestry.com. These users have been informed via email and are required to create a new password for their accounts.

If you use Ancestry.com or any of its services, here's what you can do:

Change your password - Even if you are not notified by the company, you should still change it immediately. **Check other accounts** - If you are using the same passwords for multiple accounts, change them now as well. **Beware of phishing** - Once the news of a data breach gets out, opportunistic cybercriminals try and scam unsuspecting people with phishing attacks. **Use a password manager** - You can use a third-party password manager to automatically create complex passwords for you across multiple sites.

Check your email & user name accounts at [Have I Been Pwnd](#)

APPLE SLOWING IPHONES?



Recently Apple confirmed that they have been slowing older iPhones and other devices without the knowledge of customers. Speculation circulated widely claimed it was done to push users into buying new devices.

However [Apple announced in a statement](#) that the effort was designed to prevent sudden shutdowns caused by aging batteries. Lithium-ion batteries don't last forever and regular wear and tear will diminish its performance over time (usually after two years of regular use). On an iPhone using iOS 10.2.1 or later, this notice might appear in Settings > Battery: "Your iPhone battery may need to be serviced"

Due to older batteries' diminished ability to hold a charge and supply the required voltage, iOS's "power management system" will manage the phone's load in order to maintain usability and prevent shutdowns.

As a part of Apple's apology, the company will offer anyone with iPhone 6 or later a \$50 discount on a battery replacement. Starting in January through December 2018, owners of said iPhones can have their batteries replaced for \$29.

Video Extra: [3 Tips for charging your iPhone up to 50% faster!](#)