brandprotect™

January 2016 | Briefing 13

191 MILLION VOTER RECORDS EXPOSED

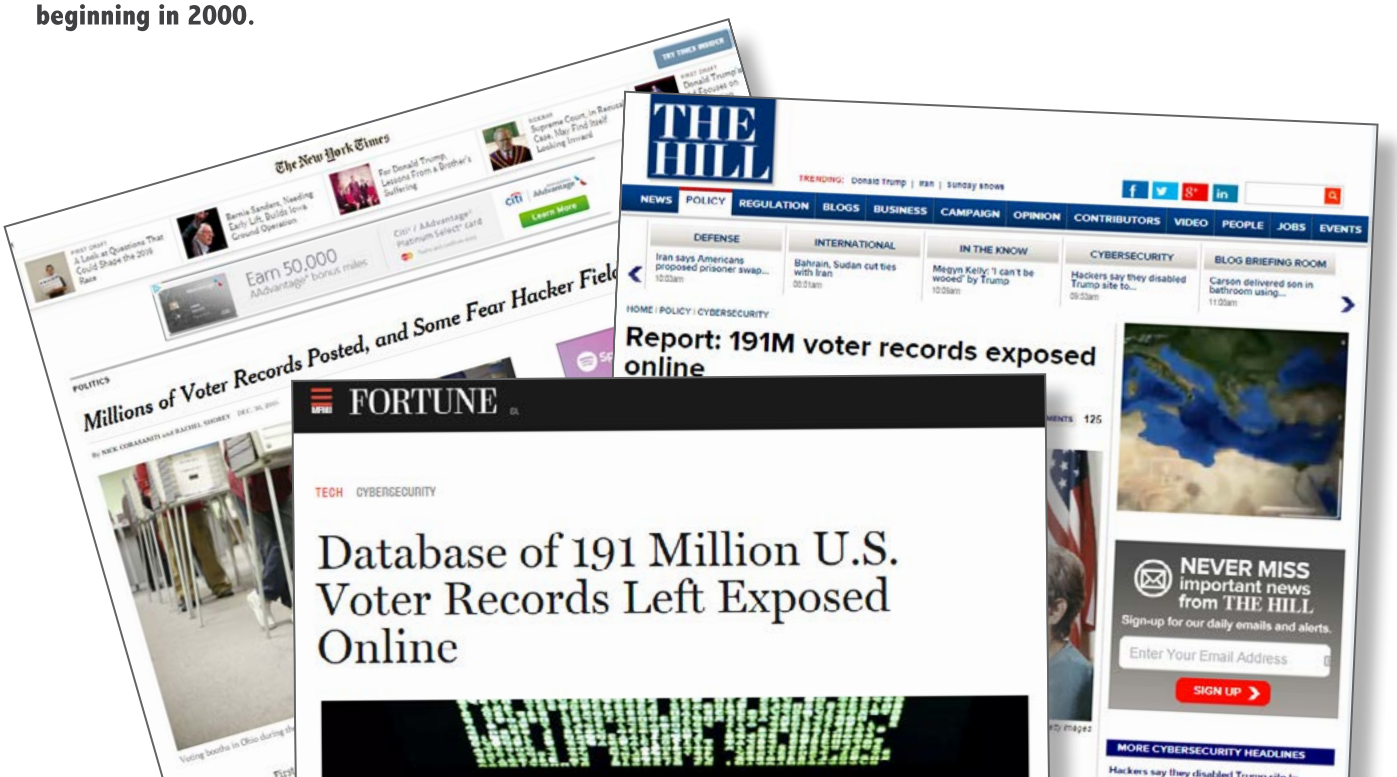
WHAT DOES IT MEAN?

Over the past weeks there has been a lot of reporting about a December 20, 2015 discovery that a database containing **191 Million voter records had been exposed online**. Because of the nature of the exposure – effectively a database containing the records was left unlocked and unprotected – there is no way to know who might have downloaded the information.

YOUR VOTING INFORMATION HAS BEEN POTENTIALLY COMPROMISED

Make no mistake, this is a big number. And it is an important number. Consider this: the US Census Bureau estimated that there were approximately 220 Million US Citizens of voting age in 2014. But not all those citizens were registered voters. The Census Bureau reports that there were 142 Million registered voters in 2014. The recent exposure of voting records is much more dramatic than a medium or large data breach. **It's effectively the exposure of PII from every registered voter in America.**

To make matters worse, the voting records database not only the basic PII for each registered voter -- full name, current mailing address, date of birth and phone number – the database also contained information about **political affiliation and voter participation in primaries and general elections beginning in 2000.**



The New York Times

POLITICS

Millions of Voter Records Posted, and Some Fear Hacker Field

THE HILL

HOME | POLICY | CYBERSECURITY

Report: 191M voter records exposed online

FORTUNE

TECH CYBERSECURITY

Database of 191 Million U.S. Voter Records Left Exposed Online

Earn 50,000
AAdvantage® bonus miles
Learn More
TRENDING: Donald Trump | Iran | Sunday shows
NEWS
POLICY
REGULATION
BLOGS
BUSINESS
CAMPAIGN
OPINION
CONTRIBUTORS
VIDEO
PEOPLE
JOBS
EVENTS
DEFENSE
Iran says Americans proposed prisoner swap...
INTERNATIONAL
Bahrain, Sudan cut ties with Iran
IN THE KNOW
Megyn Kelly: 'I can't be wooed' by Trump
CYBERSECURITY
Hackers say they disabled Trump site to...
BLOG BRIEFING ROOM
Carson delivered son in bathroom using...
NEVER MISS important news from THE HILL
Sign-up for our daily emails and alerts.
Enter Your Email Address
SIGN UP
MORE CYBERSECURITY HEADLINES

A TREASURE TROVE FOR CYBER CRIMINALS

For a cyber criminal, this is a treasure trove. **The name, address, phone #, and d.o.b data comprise the basic ingredients for identity theft and masquerading schemes**. Almost anything is possible, from the creation of counterfeit online accounts, to credit card and loan applications, backed by correct addresses and phone numbers.

But the combination of zip code and party affiliation data adds another dimension to the exposed content. Today, cyber criminals **could have access to data which can be easily correlated to reveal your likely views on social issues from tax policy, to gun control, to foreign policy, to universal health care**. There is no telling how this information might be used.

ASSUME THE WORST

It is no longer wise to pretend that "your records" might not have been exposed. You should assume they have been comprimised. Consider this: in 2015 there were 178 Million user records stolen through 780 reported data breaches at retail stores, health insurers, health care providers, government agencies, and educational institutions. **December's voting records incident (191 Million Records) exposed more PII than all of the 2015 data breaches combined**.

In 2015 there were 780 reported data breaches totaling 178 million compromised records. The voting records database incident exposed more records than all of the 2015 data breaches combined

191
MILLION
178
MILLION

WHAT SHOULD YOU DO?

There really is no simple solution to the problem of identity theft. But there are steps you can take to make reduce your exposure to attack.

1) Monitor your credit card activity: Credit Card providers are very very good at identifying unusual credit card activities, however, it pays to scrutinize your bill every month, and it is not unreasonable to review your card activity weekly, through your credit card's website. This is critically important, especially if you have provided credit cards to your spouse or your children.

2) Check your banking and brokerage accounts: Be especially wary of automated bank withdrawals -- Review your bank statements and your automated payments. Crafty criminals can sometimes create a recurring monthly payment in a small enough amount that you won't notice it. But after a few months or a year, it can amount to real money.

3) Secure every online account you can with two-factor authorization: There is no doubt that an account protected two-factor authorization is much more secure that an account protected only by a strong or very strong password. Two-factor authorization has become very common, and many sites leverage one or more of the popular account login-code generators, such as Google Authenticator

4) Migrate your day-to-day passwords to a password manager such as LastPass or Dashlane: These simple utilities will automatically generate and manage complex passwords for the sites that you frequent. Low cost subscription offerings from these companies provide you with access to you password vault from multiple authorized devices. Two-factor authorization is available to validate logins from unknown or unauthorized devices.

5) Review your online friends list at your social networking sites: Consider segmenting your contacts into those you know well, and those you are merely acquainted with. When someone asks you to make them a contact, don't say yes reflexively. Think about how you came to know them. If it is through a "mutual friend", don't hesitate to reach out to that individual to double-check the identity of your suitor.

Unfortunately, even if you are a professional at online vigilance, it does not guarantee your safety. The successful attack can come from any direction, at any time. The criminals may not make headway with you, but they will also be trying to attack someone close to you. Discuss these cyber security issues with your professional colleagues, and with your family. **Maintaining awareness of potential online attack vectors isn't fun. It takes time and effort. But the costs, of not taking action — to your family, to your friends, or to your business — can be staggering.**

SPECIAL EVENT: FREE BEST PRACTICES WEBCAST WEDNESDAY JANUARY 20TH, 2016 2 P.M. – 3.P.M. (ET)

Securing the Complex Digital Attack Surface - How Viewpost Does It

Viewpost is a leading innovator in the emerging secure transactions marketplace. To ensure the highest standards of network integrity, service trust, and reputational excellence, Viewpost is taking a leading-edge approach to security, working proactively to secure a complex external attack surface that exists far outside the traditional security perimeter.

To protect its customers, prospects and business from external cyber threat, Viewpost has implemented extensive external threat monitoring to gain visibility and actionable intelligence about illegal, infringing, and potentially damaging activities by third parties, hactivists, activists and other threat actors.

Learn from Subject Matter Experts:
Christopher Pierson, EVP, General Counsel and Chief Security Officer, Viewpost
Marc Dionne, Director of Regulatory Risk, Viewpost

Key Topics:

- How do attack surfaces change in the digital economy?
- What kinds of cyber threat monitoring and intelligence matter?
- How does Viewpost leverage internal and external resources to gain actionable cyber threat intelligence

Join this free webcast on Wednesday January 20th, 2016 2 p.m. – 3.p.m. (Eastern Time)

BrandProtect CMO, Greg Mancusi-Ungaro hosts this one-hour customer best practices webcast.

REGISTER FOR OUR WEBCAST

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

© 2016 BrandProtect Inc. All Rights Reserved.
BrandProtect and the BrandProtect logo are trademarks of BrandProtect Inc.

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.